Hur står det till med den personliga integriteten?

– en kartläggning av Integritetskommittén

Delbetänkande av Integritetskommittén

Stockholm 2016

STATENS OFFENTLIGA UTREDNINGAR

SOU 2016:41

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskanslietsförvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2016

ISBN 978-91-38-24459-3
ISSN 0375-250X

Till statsrådet Morgan Johansson

Regeringen beslutade den 8 maj 2014 att tillsätta en parlamentarisk kommitté med uppdrag att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet (dir. 2014:65). Den 18 februari 2016 beslutade regeringen tilläggsdirektiv till kommittén (dir. 2016:12) om att en del av uppdraget ska redovisas i ett delbetänkande senast den 31 maj 2016. Delbetänkandet ska enligt beslutet omfatta dels kartläggningen och analysen av riskerna för integritetsintrång, dels ett övervägande om behovet av ett integritetsskyddsråd.

Regeringen förordnade Göran Gräslund som ordförande. Sist i detta missiv finns en förteckning över förordnade ledamöter i kommittén, experter och sekreterare.

Kommittén har antagit namnet Integritetskommittén.

Integritetskommittén får härmed överlämna delbetänkandet *Hur står det till med den personliga integriteten?* (SOU 2016:41).

Arbetet i kommittén fortsätter nu med att följa upp effekterna i lagstiftningsarbetet till följd av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes år 2011. Kommittén avser också överväga förslag på åtgärder för att minska de integritetsrisker som kartlagts.

En reservation har lämnats av Agneta Börjesson och Maria Ferm (bägge MP).

Stockholm den 7 juni 2016

Göran Gräslund

Agneta Börjesson

Maria Ferm

Krister Hammarbergh

Ulf Isaksson

Eva-Lena Jansson

Ulrika Karlsson

Mathias Leveborn

Veronica Lindholm

Elin Lundgren

Jonas Millard

Andreas Norlén

Tuve Skånberg

Hanna Wagenius

Heidi-Maria Wallinder

Emanuel Öz

/Maria Jacobsson
Erik Janzon

Förteckning över ledamöter, experter och sekreterare som deltagit i utredningsarbetet samt tider för dessas förordnanden och anställningar

Ledamöter

Göran Gräslund (f.d. generaldirektör, ordförande), fr.o.m. 2014-05-18

Phia Andersson (riksdagsledamot, S), fr.o.m. 2014-06-27 t.o.m. 2015-01-21

Agneta Börjesson (riksdagsledamot, MP), fr.o.m. 2015-05-19

Christoffer Dulny (politisk sekreterare, SD), fr.o.m. 2014-06-27 t.o.m. 2014-10-19

Maria Ferm (riksdagsledamot, MP), fr.o.m. 2014-06-27

Xamuel Gonzalez Westling (kommunfullmäktigledamot V), fr.o.m. 2015-04-28 t.o.m. 2016-03-02

Krister Hammarbergh (riksdagsledamot, M), fr.o.m. 2014-06-27

Ulf Isaksson (advokat, L), fr.o.m. 2014-06-27

Eva-Lena Jansson (riksdagsledamot, S), fr.o.m. 2015-01-22

Frida Johansson Metso (leg. psykolog, L), fr.o.m. 2014-07-30[1]

Ulrika Karlsson (riksdagsledamot, M), fr.o.m. 2014-06-27

Mathias Leveborn (politisk sekreterare, V), fr.o.m. 2016-03-03

Johan Linander (f.d. riksdagsledamot, C), fr.o.m. 2014-06-27 t.o.m. 2016-03-22

Veronica Lindholm (riksdagsledamot, S), fr.o.m. 2014-10-23

Elin Lundgren (riksdagsledamot, S), fr.o.m. 2014-06-27

Jonas Millard (riksdagsledamot, SD), fr.o.m. 2014-10-20

Andreas Norlén (riksdagsledamot, M), fr.o.m. 2014-06-27

Ardalan Shekarabi (riksdagsledamot, S), fr.o.m. 2014-06-27 t.o.m. 2014-10-22

Tuve Skånberg (riksdagsledamot, KD), fr.o.m. 2014-06-27

Hanna Wagenius (jurist, C), fr.o.m. 2016-03-23

Heidi-Maria Wallinder (politisk sekreterare, V), fr.o.m. 2015-05-19

---

[1] Begäran om entledigande inlämnad.

Alice Åström (f.d. riksdagsledamot, V), fr.o.m. 2014-06-27 t.o.m. 2015-04-27

Emanuel Öz (riksdagsledamot, S), fr.o.m. 2015-05-19

Experter

Ingela Alverfors (jurist, Datainspektionen), fr.o.m. 2014-08-18 t.o.m. 2015-08-19

Fia Ewald (enhetschef, Myndigheten för samhällsskydd och beredskap), fr.o.m. 2014-06-27 t.o.m. 2016-03-22

Anne-Marie Eklund Löwinder (säkerhetschef, Internetstiftelsen i Sverige), fr.o.m. 2014-10-20

Ulrika Harnesk (jurist, Datainspektionen), fr.o.m. 2015-08-20

Anna Hörnlund (jurist, Datainspektionen), fr.o.m. 2014-06-27 t.o.m. 2014-08-17

Gunnar Idesten (it-säkerhetsspecialist, Myndigheten för samhällsskydd och beredskap), fr.o.m. 2016-03-23

Jeanette Kronwall (jurist, Post- och telestyrelsen), fr.o.m. 2014-10-20

Mårten Schultz (professor, Stockholms universitet), fr.o.m. 2014-06-27

Mathias Säfsten (ämnesråd, Justitiedepartementet), fr.o.m. 2014-06-27

Sekreterare

Maria Jacobsson, jurist, fr.o.m. 2015-11-16

Erik Janzon, enhetschef, fr.o.m. 2014-06-09

Katarina Monfils Gustafsson, dåvarande hovrättsassessor, fr.o.m. 2014-07-01 t.o.m. 2015-11-18

Innehåll

DEL I, Inledning

Sammanfattning **27**

1 Författningsförslag **35**

1.1 Förslag till förordning om ändring av förordningen (2007:975) med instruktion för Datainspektionen 35

2 Integritetskommitténs uppdrag och arbete **37**

2.1 Kommitténs uppdrag 37

2.2 Kommitténs arbete 38

2.3 Begreppet personlig integritet 39

2.4 Kommitténs bedömning av riskerna för den personliga integriteten 40

2.5 Motsvarande kartläggningar i andra länder 42
2.5.1 Norge 42
2.5.2 Danmark 43
2.5.3 Tyskland 43
2.5.4 Storbritannien 43

2.6 Betänkandets disposition 44

DEL II, Kommitténs sammantagna bedömning m.m.

3 Kommitténs sammantagna bedömning **49**

3.1 Inledning 49

3.2 Den samlade effekten för den enskilde 49

3.3 Generella problem 52
3.3.1 Kunskap om hur uppgifterna hanteras 53
3.3.2 Möjligheten för den enskilde att påverka 53
3.3.3 Den enskildes egna skyddsåtgärder 54
3.3.4 Vad tycker den enskilde? 55
3.3.5 Otillräcklig tillsyn 56
3.3.6 Sanktionerna 57
3.3.7 Globaliseringen 57
3.3.8 Journalistiska ändamål enligt personuppgiftslagen 58
3.3.9 Näthat 59
3.3.10 Offentlighetsprincipen 60
3.3.11 Personlig integritet ett viktigt värde för hela samhället 61

3.4 Teknikutvecklingen 62

3.5 Kunskapsläget 64

3.6 Drivkrafter bakom utvecklingen 65

3.7 Kommitténs bedömning av respektive område 65
3.7.1 Skolan (kapitel 7) 65
3.7.2 Arbetsliv (kapitel 8) 70
3.7.3 Hälso- och sjukvården och socialtjänsten (kapitel 9) 75
3.7.4 Forskning och statistik (kapitel 10) 77
3.7.5 E-förvaltning (kapitel 11) 78
3.7.6 Konsumentområdet (kapitel 12) 86
3.7.7 Sociala medier och e-post (kapitel 13) 89
3.7.8 Försäkringsverksamhet (kapitel 14) 91
3.7.9 Bank- och kreditmarknaden (kapitel 15) 93
3.7.10 Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso (kapitel 16) 96
3.7.11 Domstolarnas verksamhet (kapitel 17) 97
3.7.12 De brottsbekämpande myndigheternas verksamhet (kapitel 18) 100
3.7.13 Försvarsunderrättelseverksamhet och militär säkerhetstjänst (kapitel 19) 105
3.7.14 Övervakning med kamera (kapitel 20) 108
3.7.15 Molntjänster (avsnitt 21.1) 110

3.7.16 Big data (avsnitt 21.2) 114
3.7.17 Biometri (avsnitt 21.3) 115

4 Overall assessment 117

4.1 The combined impact on the individual 117

4.2 General problems 120
4.2.1 Knowledge of how data is handled 121
4.2.2 Opportunity for the individual to exert influence 121
4.2.3 The individual's own protective measures 122
4.2.4 What do individuals think? 123
4.2.5 Insufficient supervision 123
4.2.6 Sanctions 125
4.2.7 Globalisation 125
4.2.8 Journalistic purposes under the Personal Data Act 126
4.2.9 Internet hate 127
4.2.10 Principle of public access to official documents 128
4.2.11 Privacy an important value for the whole of society 129

4.3 The development of technology 131

4.4 The knowledge situation 132

4.5 Drivers behind development 133

5 Den personliga integriteten 135

5.1 Inledning 135

5.2 Teorier om personlig integritet 136
5.2.1 Inledning 136
5.2.2 Rätten att bli lämnad i fred 137
5.2.3 Oönskad tillgång till jaget 138
5.2.4 Hemlig information 138
5.2.5 Kontroll över egna uppgifter och Strömholms kränkningsförteckning 139
5.2.6 Det att vara människa 140
5.2.7 Förhållandet mellan människor 141

5.3 Behandling av begreppet i tidigare lagstiftningsarbeten 141
5.3.1 Inledning 141
5.3.2 1966 års integritetsskyddskommitté och Yttrandefrihetsutredningen 142
5.3.3 Data- och offentlighetskommittén 143
5.3.4 Skyddet för enskilda personers privatliv – En studie 144
5.3.5 Integritetsutredningen 144
5.3.6 Personuppgiftslagsutredningen 145
5.3.7 Integritetsskyddskommittén 146

5.4 Personlig integritet i detta betänkande 147
5.4.1 Begreppets innebörd 147
5.4.2 Intrång i den personliga integriteten 148

6 Det grundläggande rättsliga skyddet 151

6.1 Inledning 151

6.2 Europakonventionen 151

6.3 EU:s rättighetsstadga 152

6.4 Regeringsformen 153

6.5 Personuppgiftslagen 153
6.5.1 Dataskyddsdirektivet 153
6.5.2 Lagens tillämpningsområde 154
6.5.3 Grundläggande krav för behandlingen 154
6.5.4 Tillåten behandling 156
6.5.5 Information och rättelse 158
6.5.6 Säkerhet vid behandlingen 158
6.5.7 Överföring av personuppgifter till tredje land 159
6.5.8 Kommande lagstiftning 160

6.6 Lagen om elektronisk kommunikation 161

6.7 Tillsyn 163
6.7.1 Inledning 163
6.7.2 Datainspektionen 163
6.7.3 Övriga tillsynsmyndigheter 164
6.7.4 Pågående arbete 165

6.8 Sanktioner 165

6.8.1 Inledning 165
6.8.2 Brott mot personuppgiftslagen 165
6.8.3 Straffbestämmelser i bl.a. brottsbalken 166
6.8.4 Skadestånd 170

DEL III, Riskbedömning av olika områden och företeelser

7 Skolan 175

7.1 Inledning 175
7.1.1 Beskrivning av området 175
7.1.2 Regelverk och tillsyn 179

7.2 Digitala lärplattformar och läromedel 181
7.2.1 Företeelserna 181
7.2.2 Det skyddande regelverket 183
7.2.3 Risker för den personliga integriteten 184

7.3 Sociala medier i undervisningen 185
7.3.1 Företeelsen 185
7.3.2 Det skyddande regelverket 186
7.3.3 Risker för den personliga integriteten 187

7.4 Elevhälsan 190
7.4.1 Företeelsen 190
7.4.2 Det skyddande regelverket 191
7.4.3 Risker för den personliga integriteten 192

7.5 Skolfederationen 193
7.5.1 Företeelsen 193
7.5.2 Det skyddande regelverket 194
7.5.3 Risker för den personliga integriteten 194

7.6 Kameraövervakning i skolor 195
7.6.1 Företeelsen 195
7.6.2 Det skyddande regelverket 195
7.6.3 Risker för den personliga integriteten 196

7.7 Kommitténs samlade bedömning av området 198

8 Arbetslivet 203

8.1 Inledning 203
8.1.1 Beskrivning av området 203

8.1.2 Regelverk och tillsyn 204

8.2 Positionering 208
8.2.1 Företeelsen 208
8.2.2 Elektroniska körjournaler 208
8.2.3 Fordonskontroll 209
8.2.4 Digitala färdskrivare 209
8.2.5 Körstil 210
8.2.6 Positionering i annan utrustning 211
8.2.7 Risker för den personliga integriteten 213

8.3 Övervakning av aktiviteter och beteenden 214
8.3.1 Företeelsen 214
8.3.2 Internet och e-post 215
8.3.3 Personliga konton 216
8.3.4 Ärendehanteringssystem 217
8.3.5 In- och utpasseringssystem 218
8.3.6 Flödes- och logistiksystem 219
8.3.7 Risker för den personliga integriteten 220

8.4 Registerkontroller och medicinska undersökningar 221
8.4.1 Företeelsen 221
8.4.2 Risker för den personliga integriteten 222

8.5 Arbetstagare och sociala medier 223
8.5.1 Företeelsen 223
8.5.2 Risker för den personliga integriteten 225

8.6 Kompetensdatabaser 226
8.6.1 Företeelsen 226
8.6.2 Risker för den personliga integriteten 227

8.7 Bakgrundskontroller och kandidatdatabaser 228
8.7.1 Företeelserna 228
8.7.2 Det skyddande regelverket 231
8.7.3 Risker för den personliga integriteten 231

8.8 Kameraövervakning 232
8.8.1 Företeelsen 232
8.8.2 Det skyddande regelverket 234
8.8.3 Risker för den personliga integriteten 235

8.9 Företagshälsovård 237

8.9.1 Företeelsen ... 237
8.9.2 Det skyddande regelverket ... 238
8.9.3 Risker för den personliga integriteten ... 238

8.10 Kommitténs samlade bedömning av området ... 239

9 Hälso- och sjukvård och välfärdsteknik inom socialtjänst ... 245

9.1 Inledning ... 245
9.1.1 Beskrivning av området ... 245
9.1.2 Regelverk och tillsyn ... 246

9.2 Allmänt om hanteringen av personuppgifter inom hälso- och sjukvården ... 249
9.2.1 Informationshantering i hälso- och sjukvården ... 249
9.2.2 Hur ser informationshanteringen ut i dag? ... 250

9.3 Behörighetsstyrning, åtkomstkontroll och spärrar och annan hantering av personuppgifter inom en vårdgivares verksamhet ... 254
9.3.1 Företeelsen ... 254
9.3.2 Det skyddande regelverket ... 256
9.3.3 Iakttagelser från tillsynen ... 257
9.3.4 Risker för den personliga integriteten ... 258

9.4 Sammanhållen journalföring ... 259
9.4.1 Företeelsen ... 259
9.4.2 Det skyddande regelverket ... 260
9.4.3 Iakttagelser från tillsynen ... 260
9.4.4 Risker för den personliga integriteten ... 261

9.5 Kvalitetsregister ... 263
9.5.1 Företeelsen ... 263
9.5.2 Det skyddande regelverket ... 264
9.5.3 Iakttagelser från tillsyn och myndighetsanalyser ... 265
9.5.4 Risker för den personliga integriteten ... 267

9.6 Välfärdsteknik inom socialtjänsten ... 268
9.6.1 Används välfärdsteknik i dag? ... 268
9.6.2 Företeelsen ... 268
9.6.3 Det skyddande regelverket ... 270
9.6.4 Smers rapport om robotar och övervakning i vården av äldre ... 271

9.6.5 Risker för den personliga integriteten 272
9.7 Kommitténs samlade bedömning av området 273

10 Forskning och statistik 277

10.1 Företeelserna 277
10.1.1 Statistik 279
10.1.2 Forskning 281
10.2 Det skyddande regelverket 283
10.3 Risker för den personliga integriteten 284
10.4 Kommitténs samlade bedömning av området 288

11 E-förvaltning 291

11.1 Företeelser 291
11.1.1 Avgränsning 291
11.1.2 Ökad insamling, spridning och användning av personuppgifter 292
11.1.3 Betydelsen av att fastställa personuppgiftsansvaret 299
11.1.4 Brister i beställarkompetens 301
11.1.5 Potentiella handlingar och metadata 301
11.1.6 Offentlighetsprincipen 303
11.1.7 PSI-lagstiftningen 304
11.1.8 Eget utrymme 306
11.1.9 Medborgarprofilering 307
11.1.10 Kontroller på nätet 310
11.1.11 E-legitimation som avslöjar användaren 312
11.1.12 Myndigheter med uppgifter i molnet 313
11.1.13 Myndigheter i sociala medier och med gilla-knappar på webben 313
11.1.14 Informationssäkerhet 315
11.1.15 Regeringens mål i lagmotiv, digital agenda och e-förvaltningsstrategi 317
11.1.16 Samordning och styrning av utvecklingen 318
11.2 Det skyddande regelverket 320
11.3 Kommitténs samlade bedömning av området 321

12 Konsumentområdet 329

12.1 Inledning 329
12.1.1 Beskrivning av området 329
12.1.2 Internetekonomin 330
12.1.3 Regelverk och tillsyn 331

12.2 Kartläggning på nätet – IP-adresser, kakor och digitala fingeravtryck 333
12.2.1 Företeelserna 333
12.2.2 Sökmotorer 333
12.2.3 IP-adresser 335
12.2.4 Kakor 336
12.2.5 Digitala fingeravtryck 337
12.2.6 Det skyddande regelverket 338
12.2.7 Risker för den personliga integriteten 339

12.3 Positionering 341
12.3.1 Företeelsen 341
12.3.2 Wifi-tracking 341
12.3.3 Bluetooth low energy 343
12.3.4 RFID 345
12.3.5 GPS 347
12.3.6 Mobilnät 347
12.3.7 Det skyddande regelverket 348
12.3.8 Risker för den personliga integriteten 348

12.4 Elektroniska betalningar 349
12.4.1 Företeelsen 349
12.4.2 Det skyddande regelverket 350
12.4.3 Risker för den personliga integriteten 350

12.5 Sakernas internet (Internet of Things) 352
12.5.1 Företeelsen 352
12.5.2 Uppkopplade fordon 354
12.5.3 Det skyddande regelverket 355
12.5.4 Risker för den personliga integriteten 356

12.6 Mediekonsumtion 358
12.6.1 Företeelsen 358
12.6.2 Det skyddande regelverket 360
12.6.3 Risker för den personliga integriteten 361

12.7 Smarta mätare 361
12.7.1 Företeelsen 361
12.7.2 Det skyddande regelverket 363
12.7.3 Risker för den personliga integriteten 364

12.8 Appar 364
12.8.1 Företeelsen 364
12.8.2 Det skyddande regelverket 367
12.8.3 Risker för den personliga integriteten 367

12.9 Peer-to-peer-plattformar 368
12.9.1 Företeelsen 368
12.9.2 Det skyddande regelverket 368
12.9.3 Risker för den personliga integriteten 369

12.10 Kommitténs samlade bedömning av området 369

13 Sociala medier och e-post 373

13.1 Sociala medier 373
13.1.1 Avgränsning 373
13.1.2 Begreppet sociala medier 374
13.1.3 Olika kategorier av sociala medier 376
13.1.4 Funktioner för klagomålshantering 378
13.1.5 Annonsförsäljning 379
13.1.6 Två typer av information 379
13.1.7 Vilka har intresse för uppgifter om användarna? 382
13.1.8 Radering av uppgifter i sociala medier 385
13.1.9 Användarvillkor 385

13.2 E-post 386

13.3 Det skyddande regelverket 390

13.4 Kommitténs samlade bedömning av området 394

14 Försäkringsverksamhet 399

14.1 Om försäkring och hantering av personuppgifter 399
14.1.1 Vad är försäkring? 399
14.1.2 Behov av behandling av personuppgifter inom försäkringsföretagen 400
14.1.3 Den rättsliga regleringen 400

14.1.4 Tillsyn m.m. 401
14.1.5 Branschöverenskommelser 401

14.2 Behandling av uppgifter för att bedöma premier m.m. 402
14.2.1 Försäkring och modern teknik 402
14.2.2 Ny teknik ger nya bedömningsgrunder 403
14.2.3 Insamling av kördata 405
14.2.4 Aktivitetsmätare 405
14.2.5 Data från andra källor 406

14.3 Exempel på risker för intrång i den personliga integriteten 408
14.3.1 Dataläckage 408
14.3.2 Dataanvändning 409
14.3.3 Risk för diskriminering på försäkringsmarknaden? 409
14.3.4 Inhämtning av uppgifter om hälsa 410

14.4 Kommitténs samlade bedömning av området 412

15 Bank- och kreditmarknad 415

15.1 Allmänt om behandling av personuppgifter inom bank och kreditmarknadsföretag 415
15.1.1 Den rättsliga regleringen 416
15.1.2 Tillsyn m.m. 417

15.2 Behandling av uppgifter för kreditprövning och rådgivning 417
15.2.1 Företeelsen 417
15.2.2 Det skyddande regelverket 418
15.2.3 Risker för den personliga integriteten 419

15.3 Kreditkort och transaktioner över internet 421
15.3.1 Företeelsen 421
15.3.2 Det skyddande regelverket 422
15.3.3 Risker för den personliga integriteten 423

15.4 Behandling av uppgifter för att uppfylla rapporteringskrav m.m. 428
15.4.1 Företeelsen 428
15.4.2 Det skyddande regelverket 431

15.4.3 Risker för den personliga integriteten 432
15.5 Kommitténs samlade bedömning av området 434

16 Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso 437

16.1 Inledning 437
16.2 Kronofogdemyndigheten 437
16.2.1 Allmänt om Kronofogdemyndighetens behandling av personuppgifter 437
16.2.2 Det skyddande regelverket 439
16.2.3 Tillstånd och tillsyn 440
16.2.4 Risker för den personliga integriteten 440
16.3 Kreditupplysning 442
16.3.1 Allmänt om kreditupplysning 442
16.3.2 Det skyddande regelverket 443
16.3.3 Tillstånd och tillsyn 445
16.3.4 Risker för den personliga integriteten 446
16.4 Inkasso 450
16.4.1 Allmänt om inkassoverksamhet 450
16.4.2 Det skyddande regelverket 451
16.4.3 Tillstånd och tillsyn 451
16.4.4 Risker för den personliga integriteten 451
16.5 Kommitténs samlade bedömning av området 452

17 Domstolarnas verksamhet 455

17.1 Inledning 455
17.1.1 Om domstolarna 455
17.1.2 Domstolarnas användning av informationsteknik 456
17.1.3 Den rättsliga regleringen 457
17.1.4 Tillsyn 459
17.2 Behandling av uppgifter i verksamhetsregister och besöksterminaler 459
17.2.1 Företeelsen 459
17.2.2 Det skyddande regelverket 459

17.2.3 Risker för den personliga integriteten 460

17.3 Behandling av uppgifter i ljud- och bildupptagning 461
17.3.1 Företeelsen 461
17.3.2 Det skyddande regelverket 462
17.3.3 Risker för den personliga integriteten 463

17.4 Informationsutbyte mellan domstolar och andra myndigheter 464
17.4.1 Företeelsen 464
17.4.2 Det skyddande regelverket 464
17.4.3 Risker för den personliga integriteten 465

17.5 Utlämnande av uppgifter på medium för automatiserad behandling 466
17.5.1 Företeelsen 466
17.5.2 Det skyddande regelverket 466
17.5.3 Risker för den personliga integriteten 467

17.6 Kommitténs samlade bedömning av området 469

18 De brottsbekämpande myndigheternas verksamhet 473

18.1 Inledning 473
18.1.1 De brottsbekämpande myndigheternas användning av informationsteknik 473
18.1.2 Allmänt om den rättsliga regleringen 474
18.1.3 Tillsyn 476

18.2 Hemlig rumsavlyssning och annan ljudupptagning som inte avser elektronisk kommunikation 477
18.2.1 Företeelsen 477
18.2.2 Det skyddande regelverket 477
18.2.3 Risker för den personliga integriteten 479

18.3 Hemlig kameraövervakning och annan bildupptagning 480
18.3.1 Företeelsen 480
18.3.2 Det skyddande regelverket 480
18.3.3 Risker för den personliga integriteten 482

18.4 Hemlig avlyssning av elektronisk kommunikation 483
18.4.1 Företeelsen 483
18.4.2 Det skyddande regelverket 483

18.4.3 Risker för den personliga integriteten 486

18.5 Hemlig övervakning av elektronisk kommunikation 487
18.5.1 Företeelsen 487
18.5.2 Det skyddande regelverket 487
18.5.3 Risker för den personliga integriteten 492

18.6 Genomsökning och kopiering av mobiltelefoner och datorer 496
18.6.1 Företeelsen 496
18.6.2 Det skyddande regelverket 496
18.6.3 Risker för den personliga integriteten 498

18.7 Polismyndighetens informationsinhämtning på internet m.m. 499
18.7.1 Företeelsen 499
18.7.2 Det skyddande regelverket 499
18.7.3 Risker för den personliga integriteten 500

18.8 Tillgång till uppgifter i flygbolagens databaser (Passenger Name Record, PNR) och i EU:s informationssystem för viseringar (VIS) 501
18.8.1 Företeelsen 501
18.8.2 Det skyddande regelverket 501
18.8.3 Risker för den personliga integriteten 502

18.9 Polisens behandling av personuppgifter i register och databaser 503
18.9.1 Företeelsen 503
18.9.2 Det skyddande regelverket 503
18.9.3 Risker för den personliga integriteten 507

18.10 Internationellt informationsutbyte 512
18.10.1 Företeelsen 512
18.10.2 Det skyddande regelverket 513
18.10.3 Risker för den personliga integriteten 515

18.11 Kommitténs samlade bedömning av området 516

19 Försvarsunderrättelseverksamhet och militär säkerhetstjänst 523

19.1 Inledning 523

19.1.1 Allmänt om verksamheten 523
19.1.2 Den rättsliga regleringen 524
19.1.3 Tillsyn m.m. 525

19.2 Försvarets radioanstalts behandling av uppgifter i försvarsunderrättelseverksamhet (signalspaning) 526
19.2.1 Företeelsen 526
19.2.2 Det skyddande regelverket 527
19.2.3 Risker för den personliga integriteten 529

19.3 Försvarsmaktens informationshantering i försvarsunderrättelseverksamhet- och militär säkerhetstjänst 534
19.3.1 Företeelsen 534
19.3.2 Det skyddande regelverket 534
19.3.3 Risker för den personliga integriteten 536

19.4 Kommittén samlade bedömning av området 537

20 Övervakning med kamera 541

20.1 Inledning 541
20.1.1 Allmänt om kameraövervakning m.m. 541
20.1.2 Den rättsliga regleringen 542
20.1.3 Tillsyn 547

20.2 Användningen av övervakningskameror och därmed jämförbar utrustning 547
20.2.1 Företeelsen 547
20.2.2 Risker för den personliga integriteten 549

20.3 Lagring och automatisk bildanalys 552
20.3.1 Företeelsen 552
20.3.2 Risker för den personliga integriteten 556

20.4 Kommitténs samlade bedömning av området 557

21 Några särskilda företeelser 561

21.1 Molntjänster 561
21.1.1 Företeelsen 561
21.1.2 Det skyddande regelverket 566
21.1.3 Kommitténs samlade bedömning av området 571

21.2 Big data 575
21.2.1 Företeelsen 575
21.2.2 Det skyddande regelverket 579
21.2.3 Kommitténs samlade bedömning av området 581

21.3 Biometri 583
21.3.1 Företeelsen 583
21.3.2 Det skyddande regelverket 587
21.3.3 Kommitténs samlade bedömning av området 588

DEL IV, Övrigt

22 Informationssäkerhet och integritet 593

22.1 Inledning 593

22.2 Informationssäkerhet som område 594

22.3 Det skyddande regelverket 595

22.4 Lägesbild över informationssäkerheten i Sverige 597

22.5 Informationssäkerhet och integritet 599
22.5.1 Relationen mellan informationssäkerhet och integritet 599
22.5.2 Risker för integriteten ur ett informationssäkerhetsperspektiv 601
22.5.3 Ett europeiskt perspektiv på informationssäkerhet och integritet 606
22.5.4 Inriktning för informationssäkerheten i Sverige ur ett integritetsperspektiv 607

22.6 Tillsyn och informationssäkerhet 610

22.7 Kommitténs samlade bedömning av området 611

23 Vilket skydd erbjuder samhället den enskilde? 613

23.1 Inledning 613

23.2 Tillsyn 616
23.2.1 På vilket sätt kan tillsyn ge ett skydd? 616
23.2.2 Fungerar tillsynen? 618

23.3 Ekonomisk ersättning 622

23.3.1 På vilket sätt kan ekonomisk ersättning vara ett skydd? ... 622
23.3.2 Möjligheten för den enskilde att begära ersättning ... 625
23.3.3 Ersättningsbeloppen vid rätt till skadestånd med stöd av personuppgiftslagen ... 627
23.3.4 Fungerar ersättningssystemet i dag? ... 629
23.4 Straffrättsliga sanktioner ... 631
23.4.1 På vilket sätt kan straffrättsliga åtgärder vara ett skydd? ... 631
23.4.2 Fungerar straffrättssystemet i dag? ... 634
23.5 Kommitténs samlade bedömning ... 635

DEL V, Kommitténs förslag

24 Förslag om ökad information till regering och riksdag ... 641
24.1 Integritetskommitténs uppdrag ... 641
24.2 Integritetsskyddskommitténs överväganden ... 642
24.3 En snabb utveckling ... 643
24.4 I Norge och Tyskland ... 645
24.5 Kommitténs överväganden och förslag ... 646
24.5.1 Behovet av ett nytt organ för säkrare avvägning i lagstiftningen ... 646
24.5.2 Behovet av överblick och rapportering om utvecklingen ... 647
24.5.3 Rapport till regeringen ... 648
24.5.4 Skrivelse till riksdagen ... 649
24.5.5 Uppdraget att redovisa utvecklingen ... 650
24.5.6 Inget rådgivande organ vid Datainspektionen ... 652
24.5.7 Kostnader ... 654

25 Konsekvenser av våra förslag ... 657
25.1 Inledning ... 657
25.2 Ekonomiska konsekvenser ... 657
25.3 Andra konsekvenser ... 658

DEL VI

Ett dygn med familjen Svenssons elektroniska spår **659**

DEL VII

Reservation **691**

Bilagor

Bilaga 1 Kommittédirektiv 2014:65 695

Bilaga 2 Kommittédirektiv 2016:12 707

Bilaga 3 Integritetsskyddande teknik 709

Bilaga 4 Digitalisering och personlig integritet 743

DEL I

Inledning

Sammanfattning

Inledning

För att kunna ta del av många fördelar med modern informationsteknik delar vi med oss av våra personuppgifter. Ibland betalar vi som vanligt, men ofta får vi betala för olika tjänster genom att dela med oss av uppgifter om oss själva och ibland också om våra vänner. Det är svårt för oss att förstå och ha en överblick över på vilket sätt våra personuppgifter samlas in, sprids och vidareanvänds. Det är i dag möjligt att behandla stora mängder uppgifter om oss på ett sätt som blir mycket närgånget. Sådana behandlingar görs inte bara av kommersiella företag utan också av myndigheter.

På vilket sätt påverkar användningen av modern teknik vår möjlighet att bestämma över vilka uppgifter om oss som andra ska få ta del av? Finns det någon möjlighet att upprätthålla en fredad sfär, som inte myndigheter, företag eller andra enskilda kan komma åt? Hur står det till med den personliga integriteten i det moderna informationssamhället?

Integritetskommitténs uppdrag är att utifrån ett individperspektiv kartlägga och analysera risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik. I detta delbetänkande presenterar vi en översiktlig beskrivning av faktiska och potentiella integritetsrisker som var och en av oss utsätts för.

Kommitténs riskbedömning

För att göra det möjligt att jämföra de risker för den personliga integriteten som är förknippade med olika företeelser i samhället har kommittén valt att beskriva riskerna utifrån tre nivåer; viss risk, påtaglig risk eller allvarlig risk för den personliga integriteten. En riskbedömning utgår dels från sannolikheten för att ett intrång inträffar, dels från effekterna eller konsekvenserna av intrånget. Mer om hur vi har arbetat med riskbedömningen redovisas i kapitel 2.

Företeelser som är förknippade med viss risk för den personliga integriteten

När det gäller företeelser som är förknippade med den lägsta graden av risk för den personliga integriteten handlar det ibland om företeelser som sannolikt inte så många av oss blir föremål för. Det kan också vara så att det inte är så många uppgifter som behandlas eller att det inte är så känsliga eller närgångna uppgifter. Det kan också vara så att det finns en bra och tydlig lagstiftning och att det inte har uppmärksammats särskilt stora tillämpningsproblem. Men dessa företeelser är ändå förknippade med risker för den personliga integriteten.

De företeelser som kommittén bedömt som förknippade med vissa risker för den personliga integriteten är:

- Hanteringen av personuppgifter inom elevhälsan (skolan)
- Skolfederation (skolan)
- Arbetsgivares granskningar av vad arbetstagare skriver på sociala medier (arbetsliv)
- Kompetensdatabaser och bakgrundskontroller inom arbetslivet
- När vårdgivare tillhandahåller både hälso- och sjukvård och personaladministrativa tjänster (arbetsliv)
- Statlig statistikverksamhet (forskning och statistik)
- Myndigheters användning av sociala medier (e-förvaltning)
- Kronofogdemyndighetens verksamhet

- Inkassobolagens verksamhet
- Personuppgiftsbehandling i domstolarnas verksamhetsregister, i samband med ljud- och bildupptagningar och i samband med informationsutbyte med andra myndigheter
- Tvångsmedel med stöd av 27 kap. rättegångsbalken (brottsbekämpning)[1]
- Polisens spaningsverksamhet på internet och utåtriktade verksamhet i sociala medier (brottsbekämpning)
- Polisens hantering av personuppgifter som överförs av flygbolag och polisens deltagande i internationellt samarbete (brottsbekämpning)
- Behandling av personuppgifter i den militära underrättelsetjänstens it-system[2]

Företeelser som är förknippade med påtaglig risk för den personliga integriteten

När det gäller företeelser som är förknippade med den högre graden av risk för den personliga integriteten handlar det ofta om företeelser som innefattar behandling av fler uppgifter om enskilda och om behandlingar som omfattar många av oss. De uppgifter som behandlas kan vara känsliga eller närgångna. Sådana företeelser är ofta reglerade, men har ibland brister i regelverket eller i tillämpningen av dessa. Kommittén har bedömt riskerna efter en sammanvägning av dessa faktorer.

- Kameraövervakning (i allmänhet och särskilt beträffande övervakning inomhus i skolan)
- Informationsdelning inom och mellan myndigheter (e-förvaltning)

[1] För de enskilda personer som blir föremål för åtgärden är intrånget i den personliga integriteten tveklöst mycket närgånget. Men ur ett riskperspektiv ska även sannolikheten för att någon blir föremål för åtgärden beaktas, liksom andra relevanta faktorer som ett fungerande regelverk och risken för oönskad spridning m.m. Kommittén bedömer därför att åtgärden utgör en viss risk för den personliga integriteten, det vill säga den lägre riskgraden.

[2] Se fotnot 1.

- Informationsutbyte med enskilda (e-förvaltning)
- Vidareanvändning av offentlig information enligt PSI-lagstiftningen (e-förvaltning)
- Oskyddad e-post
- Försäkringsföretagens verksamhet
- Kreditprövning och rådgivning samt rapporteringskrav (bank- och kreditmarknad)
- Domstolarnas utlämnande av uppgifter på medium för automatiserad behandling
- Spaningsmetoder som enbart regleras av polislagen (brottsbekämpning)
- Polisens behandling av personuppgifter i register (brottsbekämpning)
- Signalspaning (försvarsunderrättelseverksamhet och militär säkerhetstjänst)[3]
- Tekniker som involverar många och detaljerade biometriska uppgifter (biometri)

Företeelser som är förknippade med allvarlig risk för den personliga integriteten

När det gäller företeelser som är förknippade med den högsta graden av risk för den personliga integriteten handlar det ofta om företeelser som innefattar behandling av många uppgifter om enskilda och om behandlingar som omfattar stora delar av befolkningen. Det handlar också ofta om behandling av mycket känsliga eller närgångna personuppgifter. Sådana företeelser kan sakna reglering eller ha stora brister i regelverket eller i tillämpningen av dessa. Kommittén har bedömt riskerna efter en sammanvägning av dessa faktorer.

[3] För de enskilda personer som faktiskt blir föremål för granskning är intrånget i den personliga integriteten tveklöst mycket närgånget. Men ur ett riskperspektiv ska även sannolikheten för att någon blir föremål för åtgärden beaktas, liksom andra relevanta faktorer som ett fungerande regelverk och risken för oönskad spridning m.m. Kommittén bedömer därför att åtgärden utgör en påtaglig risk för den personliga integriteten, det vill säga den något högre riskgraden.

- Digitala lärplattformar och digitala läromedel (skolan)
- Vissa sociala medier (i allmänhet och särskilt beträffande användningen av sociala medier i skolans undervisning)
- Arbetsgivares positionering och annan övervakning och kontroll av arbetstagarnas aktiviteter och beteenden på arbetet
- Kameraövervakning på arbetsplatser
- Hälso- och sjukvård och välfärdstjänster inom socialtjänsten
- Viss forskning
- Myndigheter med kunddata i molnet (e-förvaltning)
- Medborgarprofilering och kontroller på internet (e-förvaltning)
- Brister i myndigheters informationssäkerhet (e-förvaltning)
- Konsumentområdet
- Försäkringsföretagens framtida verksamhet
- Användningen av kreditkort och andra digitala transaktioner (bank- och kreditmarknad)
- Kreditupplysningsföretagens verksamhet
- Lagring och vidarebearbetning av uppgifter som har samlats in med hjälp av kameraövervakning
- Publika molntjänster
- Big data

Informationssäkerhet och integritet

Vi har som enskilda personer ofta små möjligheter att påverka hur uppgifter om oss hanteras. Därför är det nödvändigt att de som hanterar våra personuppgifter tar sitt ansvar för säkerheten. Kommittén anser att det finns starka indikationer på allvarliga brister i informationssäkerheten i offentliga verksamheter. När det gäller den privata sektorn har kommittén inte tillräckligt underlag för att göra en generell bedömning. I kapitel 22 skriver vi mer om detta viktiga ämne.

Övervägande om behovet av ett integritetsskyddsråd

Vi bedömer att det saknas behov av ett nytt integritetsskyddsorgan som, på det sätt som Integritetsskyddskommittén ansåg kunde övervägas, skulle ha till huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen.

Förslag om ökad information till regering och riksdag

Kommittén lämnar förslag om att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik, ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen (kap. 24).

Vi föreslår även att regeringen i en årlig skrivelse till riksdagen ska informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet.

Ett dygn med familjen Svenssons elektroniska spår

I del VI finns en vardaglig beskrivning av några integritetsrisker som en vanlig familj kan drabbas av under ett dygn. Syftet är att på ett lättillgängligt sätt redovisa hur modern teknik påverkar den personliga integriteten.

Sammanfattningsvis

I detta betänkande redogör kommittén för behandlingen av personuppgifter inom ett antal områden som en enskild person kommer i kontakt med i olika livsskeden och gör en riskbedömning av dessa. Vi beskriver därtill några vanliga generella företeelser, som har inverkan på den personliga integriteten. Vi drar också vissa slutsatser

beträffande den samlade effekten för en enskild person av all den insamling och lagring av personuppgifter, kartläggning och övervakning som han eller hon deltar i eller blir föremål för.

Den digitala utvecklingen innebär en genomgripande förändring av samhället och enskildas livsvillkor. Personuppgifter i digital form genereras och används i allt högre grad inom alla samhällsområden. Antalet aktörer ökar, användningsområdena ökar, lagringstiderna ökar, spridningen och utbytet mellan aktörerna ökar, vidareanvändningen hos respektive aktör ökar liksom spridningen över nationsgränserna. Vi ser också att vissa stora aktörer, som en följd av utvecklingen i stort och deras egna affärsstrategier, får tillgång till en allt större mängd personuppgifter och därmed har möjlighet att teckna en alltmer komplett bild av en enskild person. Ur den enskildes perspektiv innebär utvecklingen att kunskapen om hur uppgifterna hanteras, liksom möjligheten att påverka detta, hela tiden krymper i förhållande till den ökande hanteringen av personuppgifter i samhället.

I motsvarande mån begränsas även den enskildes möjlighet att genom ett verkligt fritt val bestämma hur uppgifter om honom eller henne ska hanteras. Integritetskommitténs generella slutsats är därför att den enskilde – parallellt med den digitala utvecklingen – utsätts för stegvisa försämringar av den personliga integriteten.

Självfallet innehåller den digitala utvecklingen en enorm nyttopotential, men i det här delbetänkandet har vi fokuserat på faktiska och potentiella risker.

1 Författningsförslag

1.1 Förslag till förordning om ändring av förordningen (2007:975) med instruktion för Datainspektionen

Härigenom föreskrivs i fråga om förordningen (2007:975) med instruktion för Datainspektionen att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet.	
Myndigheten ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen (1998:204).	
Myndigheten ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.	Myndigheten ska följa, *analysera och* beskriva utvecklingen på IT-området när det gäller frågor som rör integritet, ny teknik *och de legala förutsättningarna för integritetsskyddet samt årligen till regeringen lämna en redovisning om utvecklingen inom området*.

Denna förordning träder i kraft den 1 januari 2017.

2 Integritetskommitténs uppdrag och arbete

2.1 Kommitténs uppdrag

Regeringen beslutade den 8 maj 2014[1] att tillsätta en parlamentarisk sammansatt kommitté med uppdrag att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik. Inom ramen för detta arbete ska kommittén även följa upp effekterna i lagstiftningsarbetet av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes år 2011. Kommittén ska också följa upp betänkandet *Skyddet för den personliga integriteten*[2] när det gäller behovet av att inrätta ett integritetsskyddsråd samt föreslå nödvändiga författningsändringar, kopplade till denna delfråga. Det uttalas särskilt i direktivet att det i uppdraget inte ingår att föreslå ändringar i grundlag.

Uppdraget ska enligt det ursprungliga direktivet redovisas senast den 1 december 2016. Under hösten 2015 begärde kommittén en senareläggning av slutdatum till den 1 juni 2017. Regeringen beslutade i februari 2016[3] att förlänga utredningstiden enligt begäran samt att kommittén ska avge ett delbetänkande senast den 31 maj 2016, vilket ska omfatta dels kartläggningen och analysen av riskerna för integritetsintrång, dels behovet av att inrätta ett integritetsskyddsråd.

[1] Dir 2014:65.
[2] Integritetsskyddskommitténs betänkande *Skyddet för den personliga integriteten*, SOU 2008:3.
[3] Dir 2016:12.

2.2 Kommitténs arbete

Uppdraget avser personuppgiftsbehandling inom i princip alla samhällsområden. Med tanke på vidden i uppdraget var det viktigt att inledningsvis lägga fast en struktur och ett arbetssätt som både ger möjlighet till en rimlig avgränsning av uppdraget och till prioritering inom denna avgränsning. Kommittén har avstått från att fördjupa sig i områden, som andra utredningar ägnar sig åt men har däremot fortlöpande följt dessas arbete.

Vi har prioriterat områden, som hittills varit bristfälligt kartlagda, särskilt känsliga eller riskfyllda ur ett integritetsperspektiv. Vi har också inriktat oss mot ny teknik och nya tillämpningar av gammal teknik, som vi bedömer kan få en stor påverkan. En avgränsning för kartläggningen har varit att bedöma integritetsriskerna för personer som vistas i Sverige, vilket i och för sig inte utesluter att personuppgiftsbehandling utanför landets gränser till någon del omfattas av uppdraget.

Kommittén har träffats vid tolv tillfällen och sekretariatet har träffat expertgruppen vid nio tillfällen. Därutöver har sekretariatet haft samråd med utredningarna *Integritet och straffskydd* (Ju 2014:74), *Tillsynen* över den personliga integriteten (Ju 2015:02), *Mediegrundlagskommittén* (Ju 2014:07) samt haft kontakt med *Utredningen om självkörande fordon på väg* (N 2015:07).

Det i direktivet föreskrivna samrådet med Datainspektionen och Post- och Telestyrelsen har fullgjorts genom att dessa två myndigheter varit representerade i utredningens expertgrupp. Dessutom har sekretariatet haft kontakt med bl.a. Socialstyrelsen, Polisen, Försäkringskassan, Inspektionen för vård och omsorg, Skatteverket, Statens medieråd, Konsumentverket samt Datatilsynet i Norge.

För övrigt har sekretariatet genomfört ett antal expertseminarier och workshops för att fånga upp information och synpunkter från olika delar av samhället. Företrädare från hälso- och sjukvård, konsumentområdet, bank, försäkring, arbetsliv, sociala media och e-förvaltning har samlats av denna anledning. Kommittén har också genomfört en hearing med företrädare från skilda samhällsområden och professioner för att kvalitetssäkra innehållet i kapitel 3, *Kommitténs sammantagna bedömning*.

På uppdrag av kommittén har Lunds universitet genomfört en systematisk kunskapsöversikt, bestående av dels en bibliometrisk analys, dels en systematisk litteraturstudie beträffande forskningsområdet digitalisering och personlig integritet.

Kommittén har också uppdragit till konsultbyrån Kirei att ta fram en rapport, som ger exempel på tekniska, administrativa och organisatoriska åtgärder, som kan vidtas för att främja skyddet av den personliga integriteten.

Den systematiska kunskapsöversikten och rapporten om integritetsfrämjande åtgärder biläggs detta delbetänkande (bilaga 3 och 4).

Kommitténs ordförande och sekretariatet har deltagit i olika konferenser och seminarier med anknytning till utredningsuppdraget.

2.3 Begreppet personlig integritet

I likhet med ett antal tidigare utredningar om den personliga integriteten, som verkat under de senaste 50 åren, har Integritetskommittén inte funnit det meningsfullt att försöka finna en precis definition av begreppet personlig integritet. Skälet till att begreppet inte låter sig fångas i en tydlig sentens är bl.a. att rätten till en privat sfär inte är absolut. Den är relaterad till en rad olika omständigheter, som dessutom kan variera över tid. Kommittén ansluter sig därför till samma slutsats som uttrycktes i departementspromemorian *Skyddet för enskilda personers privatliv – En studie*:

> Det är svårt att ge ett sådant begrepp en tydligare avgränsning än att det innefattar vad som normalt framstår som angeläget att värna om för att den enskilde skall vara tillförsäkrad en rimlig, fredad, privat zon.[4]

En utgångspunkt för kartläggningen har därför varit den enskildes rätt till privata tankar och förtrolig kommunikation med andra, samt den enskildes möjligheter att själv avgöra vem som i olika sammanhang ska få ta del av uppgifter som rör denne. I den rätten ligger även ett skydd mot registrering, spridning eller annan behandling av felaktiga, kränkande eller påhittade uppgifter.

[4] Ds 1994:51.

Utifrån uppdraget att kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten i samband med användning av informationsteknik har kommittén fokuserat på digital insamling, användning och spridning av uppgifter – inklusive bilder – om enskilda och deras personliga förhållanden.

Kommittén ska i sin kartläggning och analys utgå från ett individperspektiv. Vi redogör därför för behandlingen av personuppgifter inom ett antal områden som en enskild person kommer i kontakt med i olika livsskeden och gör en riskbedömning av dessa. Vi beskriver därtill några vanliga generella företeelser, som har inverkan på den personliga integriteten. Vi drar också vissa slutsatser beträffande den samlade effekten för en enskild person av all den insamling och lagring av personuppgifter, kartläggning och övervakning som han eller hon deltar i eller blir föremål för.

2.4 Kommitténs bedömning av riskerna för den personliga integriteten

En traditionell riskbedömning syftar till att identifiera risker och till att därefter så långt som möjligt förhindra att riskerna leder till oönskade konsekvenser. Själva riskbedömningen innehåller dels en bedömning av sannolikheten för att en viss händelse ska inträffa, dels en bedömning av konsekvenserna av denna händelse.

I syfte att ge en mer nyanserad och förhoppningsvis användbar beskrivning av faktiska och potentiella risker för intrång i den personliga integriteten har kommittén valt att inte bara beskriva riskerna utan att också gradera riskerna i tre nivåer. Utgångspunkterna för riskbedömningen har dels varit sannolikheten för en enskild person att bli föremål för ett visst intrång, dels effekterna eller konsekvenserna av intrånget.

När det gäller att bedöma riskerna, utgår kommittén från ett antal faktorer:

- Vilken inverkan har intrånget på den enskilde? Denna inverkan är bl.a. beroende av graden av känslighet, både avseende uppgifterna som sådana men också intrångets karaktär.

- Sammanhanget och intrångets omfattning, dvs. hur många drabbas, är det fråga om stora informationsmängder, är åtgärden riktad mot en viss krets eller urskillningslös?
- Hur stor är spridningen av de uppgifter, som intrånget innebär? Här ska även risken för oönskad spridning bedömas.
- Finns ett regelverk som ska minimera riskerna för intrång? Fungerar regelverket som avsett? Efterlevs det?
- Den enskildes egen möjlighet att påverka hanteringen av personuppgifter har stor betydelse. När det gäller denna fråga är det förutom frågan om samtycke bl.a. av intresse om den enskilde har rätt till insyn i behandlingen av personuppgifter och möjligheter till rättelse vid felaktig behandling.
- Risken för att en viss behandling negativt påverkar allmänhetens förtroende i de fall den personuppgiftsansvarige till exempel är en statlig myndighet.

De olika risknivåerna benämns som **viss risk**, **påtaglig risk** och **allvarlig risk**.

Nyttan av den bedömda företeelsen vägs inte in i själva riskbedömningen. Däremot kommer nyttoaspekten att vara av central betydelse när kommittén i sitt slutbetänkande ska överväga behovet av åtgärder för att stärka skyddet av den personliga integriteten.

Följande två exempel kan illustrera vårt arbetssätt:

- Behandling av personuppgifter i samband med kreditprövning: Sannolikheten för att stora delar av befolkningen berörs är tämligen stor.[5] Det rör sig om stora informationsmängder, det finns en marknad som omsätter uppgifterna, den enskilde har inte full insyn, lagskyddet fungerar inte fullt ut. Effekterna av intrånget är därmed tämligen stora. Slutsatsen blir **påtaglig risk** för den personliga integriteten.

[5] Ur ett individperspektiv innebär det att sannolikheten är stor för den enskilde att beröras av företeelsen.

- Hemlig rumsavlyssning:
  Sannolikheten är låg för att företeelsen drabbar många. Det är fråga om ett mycket starkt intrång, men det är låg spridning av uppgifterna utanför brottsbekämpningen. Området är hårt reglerat. Beslut av domstol förutsätts. Det har inte framkommit uppgifter om att regelverket missbrukas. Här blir slutsatsen **viss risk** för den personliga integriteten.

Man skulle naturligtvis med viss rätt kunna argumentera för att intrång av det här slaget alltid ska betraktas som allvarliga. Men i en riskbedömning gäller det att inte bara gradera själva intrånget i den aktuella företeelsen, utan också hur skyddet fungerar med hänsyn till regelverk, teknisk och administrativ säkerhet etc.

Riskbedömningen ger kommittén ett bättre och mer nyanserat underlag inför det fortsatta arbetet, då kommittén ska överväga behovet av åtgärder.

2.5 Motsvarande kartläggningar i andra länder

Även i andra länder har det på senare år gjorts analyser av situationen för den personliga integriteten.

Några med Sverige jämförbara länder där sådana analyser har gjorts, är Norge, Danmark, Tyskland och Storbritannien.

2.5.1 Norge

I Norge tillsatte regeringen i maj 2007 den s.k. *Personvernkommisjonen*. Kommissionen skulle bl.a. ge en helhetsbild över vilka utmaningar som integritetsskyddet stod inför och lämna vissa förslag till åtgärder. I sitt slutbetänkande konstaterar kommissionen bl.a. att de moderna systemen för övervakning gör att övervakningen blir så omfattande att den i enskilda fall är av totalitär karaktär.[6]

Personvernkommisjonens förslag behandlades några år senare i en skrivelse från Norges regering till Stortinget.[7]

[6] Personvernkommisjonens slutbetänkande *Individ og integritet – Personvern i det digitale samfunnet*, NOU 2009:1.

[7] *Personvern – utsikter og utfordringar,* Melding til Stortinget 11 (2012–2013).

2.5.2 Danmark

Med anledning av den s.k. Se och Hör-affären i Danmark, tillsattes år 2014 två parlamentariska arbetsgrupper i Folketinget, varav den ena behandlade frågor om datasäkerhet. Arbetsgruppen skulle granska skyddet för integritetskänsliga personuppgifter i samhället i stort. Arbetsgruppens rapport innehåller inte någon kartläggning av integritetsrisker, men ger däremot en rad förslag till åtgärder för att förbättra situationen för den personliga integriteten. Förslagen rör principer for dataskydd, tillsynen över dataskyddslagstiftningen, tillsynsmyndigheternas sanktionsmöjligheter, ett samlat ansvar för dataskyddsfrågor och tekniska krav på skyddet av integritetskänsliga uppgifter.[8]

2.5.3 Tyskland

Den tyska Förbundsdagen, Bundestag, tillsatte år 2010 en undersökningskommission på temat ”internet och det digitala samhället”. En projektgrupp inom kommissionen granskade särskilt frågor om bl.a. dataskydd. Dessa frågor redovisades år 2012 i delbetänkandet *Datenschutz, Persönlichkeitsrechte, Fünfter Zwischenbericht der Enquete-Kommission Internet und digitale Gesellschaft*.[9]

I delbetänkandet ges en beskrivning av olika internetrelaterade företeelser samt lämnas en rad olika förslag. Bl.a. sägs att även om dataskyddet förändras i takt med samhället, gäller fortfarande den enskildes rätt till självbestämmande över sina uppgifter. Den rätten utgör enligt kommissionen en grundläggande beståndsdel i ett fritt och demokratiskt samhälle.

2.5.4 Storbritannien

Den brittiska dataskyddsmyndigheten, Information Commissioner’s Office, publicerade år 2006 *A Report on the Surveillance Society*.[10] Rapporten innehåller bl.a. beskrivningar av en rad vardagliga situa-

[8] *Beretning om datasikkerhed*, Beretning afgivet af Retsudvalget den 15. januar 2015 Retsudvalget 2014–15, REU Alm.del Bilag 149.

[9] Deutscher Bundestag, Drucksache 17/8999, 17. Wahlperiode 15. 03. 2012.

[10] *A Report on the Surveillance Society*, For the Information Commissioner by the Surveillance Studies Network, september 2006. Rapporten var riktad till det brittiska parlamentet.

tioner som en tänkt familj kan hamna i och som innebär någon form av kartläggning eller övervakning. I en sammanfattning av rapporten sägs bl.a. att övervakningssamhället (eng. *surveillance society*) var ett faktum redan år 2006, eftersom vardagen i världens rika länder dygnet runt präglas av kartläggning och övervakning. Även fördelarna med detta måste emellertid beaktas, konstateras det i rapporten.

Information Commissioner's Office gav år 2010 ut en uppdatering av 2006 års rapport.[11]

2.6 Betänkandets disposition

Kommittén ska enligt tilläggsdirektivet redovisa kartläggningen och analysen av riskerna för integritetsintrång och ställningstagandet till behovet av att inrätta ett integritetsskyddsråd i ett delbetänkande. Riskerna för integritetsintrång ska enligt vårt uppdrag redovisas utifrån ett individperspektiv. Vi har valt att beskriva riskerna för den enskilde individens integritet i olika samhällssektorer och även i samband med olika företeelser som är särskilt intressanta ur integritetssynpunkt.

Betänkandet är uppdelat i åtta delar (I–VIII).

Del I *Inledning* omfattar Sammanfattning, Författningsförslag (kapitel 1) och Kommitténs uppdrag och arbete (kapitel 2).

Del II *Kommitténs sammantagna bedömning m.m.* omfattar kapitel 3–6. Denna del inleds med ett kapitel om *Kommitténs sammantagna bedömning* (kap. 3) där kommittén redovisar sin bedömning av den samlade effekten av den kartläggning och övervakning som en enskild person blir föremål för i dagens alltmer digitaliserade samhälle. I kapitlet behandlas även de generella problem som vi har kunnat se griper över flera samhällsområden. Vi återger här också de sammanfattande bedömningarna som vi har gjort av de olika områden som behandlas i varje kapitel i delbetänkandet. Kapitel 4 är en engelsk sammanfattning av den generella bedömningen i kapitel 3. Kapitel 5 och 6 är två kapitel med grundläggande information om den personliga integriteten och den rättsliga regleringen.

[11] *Information Commissioner's report to Parliament on the state of surveillance*, Information Commissioner's Office, november 2010.

Del III *Riskbedömning av olika områden och företeelser* omfattar kapitel 7–21. I kapitlen redogör kommittén för vilka särskilda risker för den personliga integriteten som är förknippade med olika sektorer och företeelser i samhället. I varje kapitel gör kommittén en bedömning av riskerna för den personliga integriteten.

Del IV Övrigt omfattar kapitel 22–23, kapitel 22 handlar om informationssäkerhet och på vilket sätt ett sådant säkerhetsarbete kan skydda den personliga integriteten. I kapitel 23 beskriver kommittén vilket skydd som samhället erbjuder mot intrång i den personliga integriteten.

Del V *Kommitténs förslag* omfattar kapitel 24 och 25. I kapitel 24 tar kommittén ställning till frågan om integritetsskyddsråd och föreslår bl.a. att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen. Det sista kapitlet (25) utgör en konsekvensanalys av kommitténs förslag.

Del VI *Ett dygn med familjen Svenssons elektroniska spår* utgör en vardaglig beskrivning av vilka integritetsrisker som en vanlig familj kan drabbas av under ett dygn. Syftet är att på ett mer lättillgängligt sätt redovisa hur modern teknik påverkar den personliga integriteten.

Del VII består av en reservation till betänkandet.

Till delbetänkandet hör fyra bilagor, som presenteras i del VIII; kommittédirektiven (bilaga 1 och 2), en systematisk kunskapsöversikt beträffande forskningsområdet digitalisering och personlig integritet (bilaga 3) och en rapport, som ger exempel på olika tekniska, administrativa och organisatoriska åtgärder, som kan vidtas för att främja skyddet av den personliga integriteten (bilaga 4).

DEL II

Kommitténs sammantagna bedömning m.m.

3 Kommitténs sammantagna bedömning

3.1 Inledning

I det här kapitlet gör Integritetskommittén en bedömning av den samlade effekten för en enskild person av all den övervakning, kartläggning och lagring av personuppgifter, som han eller hon blir föremål för i dagens alltmer digitaliserade samhälle.

Vi behandlar även de generella problem som vi har kunnat se griper över flera samhällsområden.

Vi återger här också de sammanfattande bedömningarna som vi har gjort av de olika områden som behandlas i egna kapitel i delbetänkandet.

I slutbetänkandet avser vi undersöka vilka åtgärder som skulle kunna vidtas för att motverka risker som vi har identifierat. Då kan även annat än förslag till lagstiftning bli aktuellt, som exempelvis att det skulle behövas branschöverenskommelser eller proaktiva åtgärder från tillsynsmyndigheterna.

3.2 Den samlade effekten för den enskilde

I kapitel 5, *Den personliga integriteten*, beskriver vi hur vi använder oss av begreppet personlig integritet. Något förenklat förstår vi personlig integritet som allt som normalt framstår som angeläget att värna om för att den enskilde ska vara tillförsäkrad en rimlig, fredad, privat sfär. Det är vårt uppdrag att ur ett individperspektiv visa på vilken samlad effekt den senaste tidens teknik- och samhällsutveckling har haft på enskildas personliga integritet.

Utvecklingen kallas ibland för ”den digitala revolutionen”, att jämföra med den industriella revolutionen, eller för den ”tredje industriella revolutionen”, att jämföra med mekaniseringen och utvecklingen av ångkraften samt därpå med utvecklingen av elektriciteten och förbränningsmotorer.[1]

Oavsett vilken beteckning och närmare beskrivning som väljs, innebär utvecklingen en genomgripande förändring av samhället och enskildas livsvillkor. Det ligger naturligtvis en enorm nyttopotential i den här utvecklingen, men kommitténs uppdrag är att fokusera på faktiska och potentiella risker för den personliga integriteten.

I dag genereras och används digitala personuppgifter i allt högre grad inom alla samhällsområden. Antalet aktörer ökar, användningsområdena ökar, lagringstiderna ökar, spridningen och utbytet mellan aktörerna ökar, vidareanvändningen hos respektive aktör ökar liksom spridningen över nationsgränserna samt möjligheterna att behandla uppgifter i realtid. Vi ser också att vissa stora aktörer, som en följd av utvecklingen i stort och deras egna affärsstrategier, får tillgång till en allt större mängd personuppgifter och därmed har möjlighet att teckna en alltmer komplett bild av en enskild person.

Den här utvecklingen beror på digitaliseringen och på ett successivt ändrat sätt att se på informationsbehandling, både inom offentlig förvaltning och inom näringslivet.

Följande förenklade bild kan beskriva utvecklingen:

- Tidigare hade organisationer ett specifikt syfte för att bygga upp ett personregister eller en databas. Nu har man en mångfald av syften.
- Förr samlade man in uppgifter för att det fanns ett tydligt behov. Nu samlas de in för att de ”kan vara bra att ha”.
- Förr så var det viktigt, bl.a. av kostnadsskäl, att hålla lagringstiderna korta. Nu ser man stora fördelar med att behålla uppgifterna.
- Förr fanns ett givet ändamål med sökningar och analyser av personuppgifter. Nu är big data och data mining en realitet.

[1] Jfr Digitaliseringskommissionens slutbetänkande, *Digitaliseringens transformerande kraft – vägval för framtiden*, SOU 2015:91, s. 68.

- Förr samlades personuppgifterna in genom en specifik registrering. Nu uppstår de mer eller mindre automatiskt genom att den enskilde agerar och använder digitala verktyg.
- Personuppgifter har i allt högre grad blivit en handelsvara.

Den här utvecklingen har kunnat ske trots att basala dataskyddsprinciper såsom skyldighet att informera, inhämta samtycke, gallra och den s.k. ändamålsprincipen fortfarande gäller.

Ur den enskildes perspektiv innebär utvecklingen att kunskapen om hur uppgifterna hanteras, liksom möjligheten att påverka detta, hela tiden krymper i förhållande till den ökande hanteringen av personuppgifter i samhället.

I motsvarande mån begränsas även den enskildes möjlighet att genom ett verkligt fritt val bestämma hur uppgifter om honom eller henne ska hanteras.

Kommitténs generella slutsats är därför att den enskilde på ett flertal områden drabbas av stegvisa försämringar av den personliga integriteten.

Vi kan konstatera en förskjutning av inflytandet över hur uppgifterna hanteras – från den enskilde till de personuppgiftsansvariga och från de personuppgiftsansvariga till tjänsteleverantörerna. Tjänsteleverantörerna är inte sällan stora globala företag, även om de i formell mening endast är personuppgiftsbiträden och därmed är skyldiga att följa de ansvarigas instruktioner. De globala företagen är mycket stora, men få till antalet, och vanligen baserade i USA. Förskjutningen innebär därför också en koncentration och en geografisk omplacering av inflytandet bort från Sveriges och EU:s jurisdiktion.

Regleringen av hur uppgifter får hanteras ligger till stora delar på EU-nivå. Det nationella inflytandet från regering och riksdag får således utövas genom EU-samarbetet med de begränsningar som detta innebär. Härtill kommer, som redan nämnts, att den verkliga hanteringen av uppgifter många gånger äger rum utanför EU, vilket i sin tur minskar EU:s möjligheter att påverka hanteringen. I sammanhanget är det av betydelse att EU:s bestämmelser om dataskydd oftast ger ett starkare skydd än motsvarande regler i andra delar i världen, exempelvis i USA.

Klart står emellertid att när kunskapen och kontrollen förhållandevis minskar, måste slutsatsen bli att situationen för den personliga integriteten försämras, egentligen oberoende av vilken definition man väljer av begreppet personlig integritet.

Den enskildes minskande självbestämmande i detta hänseende är en utmaning som staten kan förhålla sig till på olika sätt. Den kan acceptera den enskildes relativt sett krympande kunskaper och påverkansmöjligheter utan vidare. Den kan verka för att öka enskildas kunskaper och påverkansmöjligheter. Den kan också verka för att förhindra sådan hantering av uppgifter som av något skäl inte är önskvärd. Den svenska staten har hittills valt en blandning av samtliga tre förhållningssätt.

Den samlade bilden av hur uppgifter hanteras i dag är en utmaning som också enskilda förhåller sig till på olika sätt. Situationen väcker frågan om människan och hennes beteende förändras av den accelererande digitala hanteringen av hennes uppgifter och hennes privata sfär? Och i så fall hur? Lunds universitet har på vårt uppdrag tagit fram en systematisk kunskapsöversikt om detta. Den visar att det såväl internationellt som i Sverige finns förvånansvärt lite kunskap om vilken inverkan som digital övervakning har på människans beteende och på hennes uppfattning om världen och sig själv. Vissa studier finns som pekar på att risken för bristande respekt för den personliga integriteten kan leda till minskat internetanvändande och minskat politiskt engagemang (åtminstone på nätet).[2] Men ännu saknas vetenskapligt hållbara och empiriska bevis för att så verkligen är fallet.

3.3 Generella problem

Vissa utmaningar för den personliga integriteten är inte avgränsade till någon särskild del av samhället, utan kan möta den enskilde i många olika situationer. Vi vill därför lyfta fram dessa och behandla dem särskilt, även om de sedan återkommer i olika sammanhang när vi återger de allvarligaste riskerna per område.

[2] Se de artiklar som återges i kunskapsöversikten, särskilt i avsnittet om kunskap och beteende hos unga. Det finns även andra rapporter om detta, exempelvis *Global Chilling – The Impact of Mass Surveillance on International Writers*, Results from PEN's International Survey of Writers (januari 2015).

3.3.1 Kunskap om hur uppgifterna hanteras

En återkommande iakttagelse är att enskilda i stor utsträckning är omedvetna om och har dåliga kunskaper om hur och varför deras personuppgifter hanteras i utrustningar och tjänster i olika sammanhang. Detta bekräftas av ett antal undersökningar. I en undersökning inom arbetslivsområdet angav endast 21 procent av de tillfrågade arbetstagarna att de visste vilka uppgifter som arbetsgivaren samlade in om deras internetanvändande.[3] I en annan undersökning ansåg åtta av tio tillfrågade svenskar att de inte har full kontroll över sina personuppgifter.[4] En liknande iakttagelse har kommittén gjort beträffande personuppgiftsansvariga företag eller myndigheter. Här finns inte enkätundersökningar på samma sätt som avseende enskildas kunskaper och inställning. Men i våra kontakter med olika parter och i vår omvärldsbevakning har framkommit att det inte är ovanligt med bristande kunskaper även hos de personuppgiftsansvariga. Ett tydligt exempel på detta är myndigheter som köper molntjänster utan att skaffa sig närmare kunskaper om hur uppgifterna hanteras och sprids inom tjänsten.

3.3.2 Möjligheten för den enskilde att påverka

Flera faktorer gör det svårare för den enskilde att påverka hur de egna uppgifterna lagras och sprids. Dels blir detta svårare på grund av den ökande vidareanvändningen av uppgifter för nya ändamål på olika håll i samhället, exempelvis genom big data, dels för att vi använder oss av utrustning som genererar och sprider allt fler personuppgifter, exempelvis genom appar och sensorer som finns installerade i t.ex. mobiltelefoner och fordon.

När den enskilde inte känner till och inte kan påverka hur personuppgifter hanteras, urholkas samtyckets betydelse. De samtycken som inhämtas för olika behandlingar framstår alltmer som en chimär. Även i situationer där hanteringen är glasklar för den enskilde och ett tydligt samtycke efterfrågas, kan den enskilde i praktiken sakna valmöjlighet. Det betingar ofta ett högt pris i form av att exempelvis

[3] Rapport från den 26 juni 2014 om en undersökning som fackförbundet Unionen genomförde bland sina medlemmar.

[4] Special Eurobarometer 431, Data Protection, publicerad i juni 2015 samt Datainspektionens årsredovisning för 2015, s. 4.

avstå från mediekonsumtion på nätet, från att kommunicera med hjälp av sociala nätverk, från att använda kreditkort och från kontakter med vissa vårdgivare. Människan är en social varelse och befinner sig i en teknologisk kontext som det i praktiken är mycket svårt att ställa sig utanför. Att inte samtycka innebär nämligen att stå utanför, och är därmed sällan ett realistiskt alternativ. Ofta är samtyckesfrågor binärt formulerade; antingen samtycker den enskilde till allt som den ansvarige vill göra med uppgifterna för att tillhandahålla en viss tjänst, eller så samtycker den enskilde inte och får då helt avstå från tjänsten. Graderade alternativ förekommer sällan. I vissa sammanhang, som inom den offentliga förvaltningen, finns dessutom lagstiftning som inte förutsätter samtycke för behandling av uppgifterna. Den enskilde har då inte någon laglig möjlighet att motsätta sig att uppgifterna hanteras. Detta kan få långtgående effekter när uppgifter från förvaltningssfären når privat sektor genom exempelvis molntjänster eller med stöd av offentlighetsprincipen.

3.3.3 Den enskildes egna skyddsåtgärder

Den enskildes möjlighet att vidta skyddsåtgärder förutsätter kunskap om hur uppgifter hanteras och sprids av företag och myndigheter, men också kunskap om hur uppgifter sprids av andra enskilda personer, t.ex. när bilder på enskilda personer publiceras på sociala medier av andra användare.

Det är i praktiken ofta tidsödande och krångligt att skydda sig på andra sätt än att stå utanför, t.ex. genom att använda sig av krypterad e-post eller andra tekniker som är tillgängliga för den enskilde. Det framstår därmed inte som ett realistiskt alternativ för det stora flertalet. En informationssäkerhetspecialist har på vårt uppdrag tagit fram en översikt över integritetsskyddande teknik.[5] Kommittén delar den bedömning som görs i rapporten av enskildas möjligheter att skydda sig mot intrång i den personliga integriteten:

> Många tjänster i vardagen som vilar på modern informationsteknik, och som uppfattas som oumbärliga, medför inte sällan en ingående kartläggning av individen. (…) Det går knappast som enskild medborgare att värja sig mot det integritetsintrång som sker genom användning av dessa tekniker, med mindre än att aktivt välja att inte använda flertalet av dem. Få kan nog tänka

[5] Bilaga 4.

sig att sluta köpa elektricitet eller att sluta använda en mobiltelefon. Alternativen, att som konsument försöka skydda sin privata sfär genom olika medel, blir ofta så opraktiskt och kostsamt att det aldrig står som ett reellt alternativ för andra än grovt kriminella. Denna grupp av individer kan tänkas vidta långtgående åtgärder för att undvika att lämna elektroniska fotspår, innefattande att uteslutande använda kontanter, att alltid bruka anonymiseringstjänster på internet och oregelbundet byta mellan olika mobiltelefoner och oregistrerade SIM-kort på olika platser, och också hålla apparaterna avstängda då de inte behövs.

3.3.4 Vad tycker den enskilde?

Det faktum att enskilda lämnar ifrån sig personuppgifter och inte i större utsträckning vidtar de mått och steg som ändå är möjliga för att skydda sina uppgifter, betyder inte att enskilda i allmänhet struntar i sin personliga integritet. I flera undersökningar svarar enskilda tvärtom att det är viktigt för dem hur deras uppgifter hanteras, att de önskar ett tydligt regelverk som upprätthålls och att deras förtroende för olika aktörer i detta hänseende varierar stort. I en stor europeisk undersökning år 2015 om allmänhetens inställning till personlig integritet, tog 52 procent av de svenska respondenterna avstånd från uttalandet ”att lämna ut personlig information är inget problem för dig”.[6]

I en annan undersökning, genomförd av ett fackförbund, svarade en klar majoritet av de tillfrågade medlemmarna att de inte var oroliga för integritetskränkningar i arbetslivet och att de inte heller själva hade blivit utsatta för något sådant.[7] *När de däremot fick läsa några exempel på övervakning och därefter fick ta ställning till om de tyckte att fackförbundet skulle driva frågan om stärkt* integritetsskydd, var det en lika klar majoritet som tyckte att förbundet skulle driva frågan.

[6] Special Eurobarometer 431, Data Protection, publicerad i juni 2015 samt Datainspektionens tidning *Integritet i fokus*, nr 4, 2015.

[7] Rapport från den 26 juni 2014 om en undersökning som fackförbundet Unionen genomförde bland sina medlemmar.

3.3.5 Otillräcklig tillsyn

Tillsynen av hur personuppgifter hanteras når bara en bråkdel av alla företeelser som är riskabla ur ett integritetsskyddsperspektiv. Det största tillsynsansvaret bärs av Datainspektionen, vars uppdrag i stort sett har varit detsamma sedan myndigheten bildades år 1973. Myndigheten har i dag cirka 45 årsarbetskrafter, vilka även ska utöva tillsyn över inkassoverksamhet och kreditupplysningsbranschen. Myndighetens storlek och uppdrag medför att många nya företeelser och aktörer av naturliga skäl inte alls blir granskade och bedömda ur ett integritetsskyddsperspektiv, eller blir det först när de funnits på marknaden under en period.

På senare år har situationen påverkats av att Datainspektionen successivt har minskat sina tillsynsaktiviteter. Myndigheten förklarar detta bl.a. med att antalet remisser och delningar ökat markant och att detta tagit resurser från tillsynsverksamheten.[8]

Inom det här området kan tillsynen sägas vara särskilt viktig. Nya företeelser introduceras i en mycket snabb takt. Många av dessa finns det anledning att bedöma ur ett rättsligt perspektiv. Regelverket är tämligen oprecist och avsiktligt allmänt hållet. Det är därför ofta först när tillsynsmyndigheten har bedömt en ny företeelse, som leverantörer och användare får någon ledning. Resultatet från tillsynen kan sedan användas i tillsynsmyndighetens utåtriktade och proaktiva arbete för att sprida kunskap.

Konsumentverket har uppgett sig ha vissa svårigheter med tillsynen i den digitala miljön. Problemen rör bl.a. digital och individanpassad marknadsföring på exempelvis sociala medier, som baseras på en mer eller mindre ingående profilering. Företeelsen har inte varit föremål för Konsumentverkets tillsyn. Likaså har inte användarvillkoren för sociala medier ännu granskats av Konsumentverket.

I kartläggningen har kommittén kunnat konstatera att tillsynen av den personliga integriteten i dag är splittrad på flera olika myndigheter. Förutom av Datainspektionen och Konsumentverket bedrivs tillsyn inom integritetsområdet av bl.a. Post- och telestyrelsen, Säkerhets- och integritetsskyddsnämnden och länsstyrelserna. En splittrad tillsyn kan innebära effektivitetsförluster beträffande den totala tillsynen. Vi avstår från att i nuläget fördjupa oss i frågan, eftersom den för närvarande analyseras av Utredningen om tillsynen över

[8] Datainspektionens årsredovisning för 2015, s. 4.

den personliga integriteten.[9] Utredningen ska, i syfte att stärka skyddet för den personliga integriteten, överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet.

3.3.6 Sanktionerna

Generellt för hela området är att sanktionssystemet, både det straffrättsliga och det skadeståndsrättsliga, inte verkar användas i någon större omfattning. Det är i alla fall mycket få ärenden som når domstolarna. Exempelvis har vi för perioden 2012–2015 endast funnit fem tvistemål i tingsrätt där frågan handlat om skadestånd enligt personuppgiftslagen (1998:204). Det ser inte annorlunda ut på straffrättens område. Under år 2014 avgjordes sammanlagt i landet endast fyra ärenden om brott mot personuppgiftslagen (genom domslut, strafföreläggande eller åtalsunderlåtelse).

När systemet väl används rör det sig om lindriga straff och låga skadeståndsbelopp.

Sammanfattningsvis kan sanktionssystemet inte sägas fungera fullt ut, eftersom det inte har fått den effekt som avsågs med bestämmelserna.

3.3.7 Globaliseringen

En annan generell iakttagelse är att digitala tjänster alltmer präglas av globaliseringen. Många olika aktörer i olika länder samarbetar exempelvis i tillhandahållandet av alla komponenterna och programmen i en mobiltelefon. Personuppgifter om användaren kan ibland hanteras såväl av dem som tillverkat telefonen, som av operativsystemet liksom av apparna i telefonen. De olika tillverkarna återfinns inte sällan i olika världsdelar. Apparna är i sin tur ofta molnbaserade. I molntjänsters natur ligger att data flyttas mellan olika datacenter över hela världen. Det leder också till att dessa länders lagstiftning kommer att tillämpas på hur uppgifterna får hanteras, varvid det kan röra sig om bestämmelser som ger ett väsentligt sämre skydd för uppgifterna än

[9] Ju 2015:02.

reglerna i Sverige och EU, avseende exempelvis statens rätt att ta del av uppgifterna. Hanteringen i andra länder medför också att det i praktiken oftast är omöjligt att utöva kontroll och tillsyn över hur uppgifterna verkligen hanteras.

En annan följd av globaliseringen är att när myndigheter behöver lämna ut uppgifter till företag som är etablerade i andra länder, är det därefter andra landets lagar som reglerar hur uppgifterna får hanteras och spridas vidare.[10]

3.3.8 Journalistiska ändamål enligt personuppgiftslagen

En fråga vi inte berör närmare i vår kartläggning är att dagens svenska ramlagstiftning, personuppgiftslagen, föreskriver att regelverket i väsentliga delar inte behöver tillämpas i vissa situationer eftersom det skulle begränsa yttrandefriheten. Det rör sig inte bara om publicering på nätet med hjälp av s.k. frivilliga utgivningsbevis, som ger grundlagsskydd och därmed sätter delar av personuppgiftslagen ur spel. Även en publicering utan frivilligt utgivningsbevis faller utanför personuppgiftslagens tillämpning, om publiceringen görs för ett s.k. ”journalistiskt ändamål”. Bestämmelsen har sin grund och motsvarighet i artikel 9 i dataskyddsdirektivet. När bestämmelsen har prövats av Högsta domstolen i Sverige, har domstolen bedömt att verksamhet som innebär att informera, utöva kritik och väcka debatt om samhällsfrågor av betydelse för allmänheten, ska anses ha ett journalistiskt ändamål i personuppgiftslagens mening. Det kan alltså utgöra ett journalistiskt ändamål att informera, kritisera och debattera i vissa frågor, även om man gör det på ett för enskilda personer kränkande sätt.[11]

Bestämmelsen har i tillämpningen tolkats brett och har tillämpats exempelvis på publicering på nätet i form av bloggar som innehållit personuppgifter och som uppfattats som kränkande av de personer

[10] Se t.ex. Högsta förvaltningsdomstolens avgörande HFD 2014 ref. 66 där den omständigheten att ett företag var etablerat i Norge medförde ett sämre sekretesskydd för uppgifter hos Socialstyrelsen eftersom det norska företaget inte var bundet av personuppgiftslagen. Frågan handlade om utlämnande.

[11] NJA 2001 s. 409 samt Öman & Lindblom, *Personuppgiftslagen* (15 oktober 2015, Zeteo), kommentaren till 7 § andra stycket personuppgiftslagen.

som omnämnts. Eftersom ändamålet med publiceringen befunnits vara journalistiskt, har publiceringen inte ansetts strida mot personuppgiftslagen.[12]

3.3.9 Näthat

Vad användare av sociala medier kan skriva och publicera om andra enskilda personer på nätet är en annan, betydande risk för den personliga integriteten.

De senaste åren har det allt oftare rapporterats om olika former av hatkampanjer på nätet. Företeelsen kallas ofta för *näthat*. Exempelvis framgår det av organisationens Friends senaste rapport om barns och ungdomars erfarenhet av internet, att så många som var tredje person i åldersgruppen 10–16 blivit utsatt för kränkningar på nätet under det senaste året.[13]

I alla åldersgrupper är det vanligare att kvinnor utsätts för kränkningar på nätet än män. I betänkandet *Integritet och straffskydd*[14] görs en sammanställning över forskning om kränkningar av den personliga integriteten på nätet. I sammanställningen sägs bl.a. att det finns forskare på området som menar att många hatkampanjer på internet har en tydlig könsaspekt där kvinnor utsätts för sexualiserade kränkningar i avsevärt större utsträckning än män. Enligt dessa forskare kan det i förlängningen leda till en självcensur som skulle kunna ses som ett hot mot jämställdheten och yttrandefriheten.

Näthat kan även bedrivas av organisationer. Det har exempelvis förekommit att enskilda journalister blivit utsatta för upprepade och systematiska kränkningar på nätet av organisationer som de granskar, med det tydliga syftet att få granskningen att upphöra.[15]

Nätet beskrivs ibland som en ny arena för hot och kränkningar. Genom internet och annan elektronisk kommunikation har möjligheterna för enskilda att sprida integritetskränkande uppgifter om andra ökat väsentligt. Nya skyddsintressen har därför uppkommit

[12] NJA 2001 s. 409.

[13] Friends nätrapport 2016.

[14] Utredningens om ett modernt och starkt straffrättsligt skydd för den personliga integriteten betänkande *Integritet och straffskydd*, SOU 2016:7.

[15] I media har t.ex. nyligen rapporterats om ett fall i Finland, se artikeln *Grävande journalist blev måltavla för proryska troll*, publicerad på svt.se den 13 mars 2016 och författad av Ulf Mattmar och Hedvig Eriksson.

och medfört ett väsentligt ökat behov av ett bättre utformat straffrättsligt skydd för privatlivet och den personliga integriteten. Med den motiveringen föreslås i betänkandet *Integritet och straffskydd*[16] en ny straffbestämmelse om olaga integritetsintrång i 4 kap. brottsbalken. Den föreslagna bestämmelsen innebär ett straffansvar för den som gör intrång i någon annans privatliv genom att sprida bild eller annan uppgift på ett sätt som är ägnat att medföra kännbar skada för den som uppgiften rör.

Eftersom näthat som företeelse således nyligen analyserats, och då detta även lett till att det lämnats ett förslag som syftar till att angripa problemet, avstår kommittén från att fördjupa sig i företeelsen.

3.3.10 Offentlighetsprincipen

I och med 1766 års tryckfrihetsförordning infördes offentlighetsprincipen i svensk rätt. Den stadgar att all myndighetsutövning ska vara transparent och att den som så önskar har rätt att ta del av myndigheters offentliga handlingar. Sedan införandet har offentlighetsprincipen haft en i huvudsak obruten kontinuitet och den har ett brett och starkt stöd i riksdagen. Principen utgör i dag en hörnsten för demokratin i Sverige.

Offentlighetsprincipen har handlingsoffentlighet som utgångspunkt, varifrån avsteg endast får göras i särskild ordning och efter att lagstiftaren för varje avsteg gjort en noggrann intresseavvägning mellan behovet av offentlighet å ena sidan och behovet av sekretess å andra sidan.

I takt med digitaliseringen uppkommer nya konsekvenser för offentlighetsprincipen. Ju bättre och billigare de tekniska möjligheterna att sprida och sambearbeta olika uppgifter blir, desto större blir det kommersiella värdet av de personuppgifter som finns hos myndigheterna. Många företag vill därför få åtkomst till uppgifterna. En del myndigheter kan ta betalt för vissa utlämnanden. Uppgifterna får därmed en ekonomisk betydelse även för myndigheterna. När företag har fått ut uppgifter med stöd av offentlighetsprincipen, kan de sprida och hantera uppgifterna för helt andra ändamål än dem för vilka myndigheten ursprungligen samlade in uppgifterna. Ibland kan företagen även publicera integritetskänsliga uppgifter på nätet med

[16] SOU 2016:7.

grundlagsskydd genom s.k. frivilliga utgivningsbevis, med den följden att vissa delar av det integritetsskyddande regelverket inte längre gäller. Frågan om de frivilliga utgivningsbevisens innebörd för den personliga integriteten, är för närvarande föremål för utredning i Mediegrundlagskommittén.[17]

Den svenska offentlighetsprincipen och det europeiska dataskyddsregelverket kan sägas verka i olika riktningar på ett principiellt plan: offentlighetsprincipen har offentlighet som utgångspunkt (och sekretessbestämmelser som reglerar undantagen), medan dataskyddsdirektivets huvudregel är att personuppgifter inte får spridas (om inte spridningen har stöd i någon av direktivets bestämmelser). Kommittén bedömer dock att de principiella skillnaderna har kunnat hanteras i den praktiska tillämpningen.

3.3.11 Personlig integritet ett viktigt värde för hela samhället

Det är inte bara för individen som den personliga integriteten är av betydelse. Även för samhället i stort är det avgörande att invånarna kan vara fria i sin åsiktbildning och i sina yttranden samt att de som utgångspunkt kan ägna sig åt vad de vill och umgås med vem de vill, utan inblandning och insyn från utomstående. Rätten till personlig integritet (som i sig är en grundlagsskyddad mänsklig rättighet) är därmed en viktig faktor även för andra, centrala och grundlagsskyddade rättigheter, dvs. för sådana rättigheter som är grunden för ett demokratiskt samhälle, särskilt rätten till yttrandefrihet, men även rätten till informationsfrihet och meddelarfrihet.

Vi har de senaste åren sett flera exempel på kränkningar av enskilda personer i syfte att tysta dem i deras opinionsbildning, politiska verksamhet eller journalistiska granskningsarbete. Om det här slaget av kränkningar av våra grundläggande rättigheter får sådana effekter att det på bredden påverkar enskildas vilja att kommunicera sin mening och delta i det offentliga samtalet, innebär det ett hot mot demokratin.

På samma sätt kan grundläggande värden hotas om enskilda avstår från aktiviteter på grund av förlorad tillit eller oro för att de ska bli registrerade, kartlagda eller övervakade på ett sätt som på sikt skulle kunna skada dem.

[17] Ju 2014:17.

Det finns inget tvivel om att det i enskilda fall finns personer som har valt att avstå från att utnyttja sina rättigheter, efter att ha utsatts för diverse kränkningar, hot och påtryckningar. Kommittén har dock inte underlag för att säkert kunna fastställa att befolkningen i stort har påverkats i sitt beteende med anledning av en ökad oro för att bli angripen på nätet, kartlagd eller övervakad.

Ett annat rättighetsrelaterat problem är den massiva datainsamling som möjliggör profilering och individanpassad marknadsföring eller individanpassade sökresultat (uppkomsten av s.k. filterbubblor)[18], vilket kan leda till diskriminering och exkludering i strid med 1 kap. 2 § regeringsformen.

Ytterligare en risk består i ett eventuellt framtida, men långt ifrån omöjligt, scenario där mänskliga rättigheter inte längre upprätthålls på samma sätt som i dag, i Sverige eller i länder som vi samarbetar med och till vilka uppgifter flödar relativt fritt. De stora möjligheter som finns för myndigheter och företag att kartlägga enskilda, kan då komma att användas på sätt som kan vara mycket negativa för den enskilde.

3.4 Teknikutvecklingen

I vår granskning har vi särskilt noterat vissa företeelser av mer teknisk natur som återkommer inom flera områden. Dessa företeelser ökar rent generellt i användning. Enligt vår mening är de av stor betydelse för integritetsskyddet redan i dag, men kan förväntas få ännu större betydelse i en inte alltför avlägsen framtid. De kan även komma att rita om spelplanen på flera sätt.

Big data och sakernas internet (Internet of things) är två sådana företeelser som vi behandlar i delbetänkandet.[19]

[18] Företeelsen beskrivs närmare i kapitel 12 om konsumentområdet.
[19] Kapitel 21 om några särskilda företeelser och kapitel 12 om konsumentområdet.

Två andra företeelser är av ännu mer teknisk natur, men kommer att förändra förutsättningarna för hur vi kan hantera personuppgifter i framtiden: utvecklingen av artificiella neurala nätverk[20] och utvecklingen av kvantdatorn[21].

Vi har också noterat att vissa företeelser inte har fått den betydelse för den personliga integriteten som de en gång förutspåddes få. Ett exempel på detta är RFID-taggar som vi visserligen nämner som en möjlig risk för den personliga integriteten, men som för några år sedan förväntades få betydligt större konsekvenser för den personliga integriteten än vad vi bedömer att den faktiskt har fått. Det visar att det är svårt att med någon större exakthet förutspå vilka företeelser som kommer ha störst genomslag och inverkan även inom en nära framtid.

En annan iakttagelse som vi har gjort är att integritetsskyddande teknik skulle kunna användas i betydligt större omfattning än vad som är fallet i dag. Flera goda exempel tas upp i den tidigare nämnda översikten.[22] Översikten har som utgångspunkt bl.a. att användandet av väl utformad integritetsfrämjande teknik gör det möjligt att uppnå en mer fördelaktig jämvikt i avvägningen mellan nyttoeffekter och risker för den personliga integriteten. Detta är enligt vår mening ett tydligt förbättringsområde.

En annan genomgående iakttagelse är att staten inte har någon helhetsbild över utvecklingen i stort på det här området, varken när det gäller teknikutvecklingen eller när det gäller nya arbetssätt som involverar personuppgiftsbehandling. Staten har enligt flera gransk-

[20] Nationalencykopedin förklarar neurala nätverk som nätverk av enkla summerande enheter som kommunicerar via kopplingar. I biologiska neuronnätverk är enheterna nervceller (neuroner) och kopplingarna synaptiska förbindelser. Biologiska neuronnätverk har utgjort förebilder vid utvecklingen av artificiella neuronnätverk, vilka realiseras som datorprogram, som integrerade kretsar (neurochips) eller med hjälp av analog optisk teknik, t.ex. holografi. Utmärkande för artificiella neuronnätverk är bl.a. inlärningsförmåga, parallellitet som medger hög beräkningshastighet och robusthet med avseende på felaktigheter och brus i indata och i nätverket självt. Exempel på användningsområden för neurala nätverk är mönster- och bildigenkänning, medicinska prognoser och artificiell intelligens.

[21] Enligt Nationalencykopedin är den stora skillnaden mellan en vanlig dator och en kvantdator, att en sträng av kvantbitar i en kvantdator kan befinna sig i en (koherent) överlagring av alla kvantbitar som ingår i strängen, s.k. parallellism. Kvantbitarna kan också vara hoptvinnade, vilket medger mycket speciella möjligheter för en kvantdator att utföra beräkningar. Det är dessa två egenskaper, parallellism och framför allt hoptvinning, som ger en kvantdator dess unika egenskaper jämfört med en vanlig dator. En kvantdator kan inte utföra andra beräkningar än en vanlig dator, bara på ett annat sätt, men skulle kunna utför vissa beräkningar mycket snabbare än en vanlig dator.

[22] Bilaga 4.

ningsrapporter inte heller en samlad överblick och kontroll över hur den egna förvaltningen utvecklas inom området, dvs. inom den statliga e-förvaltningen.

3.5 Kunskapsläget

Flera generalla iakttagelser görs i den tidigare nämnda kunskapsöversikten från Lunds universitet beträffande kunskapsbildningen på forskningsområdet digitalisering och personlig integritet.[23] Vi tror att deras iakttagelser har betydelse även utanför de akademiska miljöerna och återspeglar generella tendenser.

Översikten visar att det råder en tämligen strikt indelning av forskningen om digitalisering och personlig integritet mellan huvudsakligen tre vetenskapliga fält. Det första är ett tekniskt fält som i hög grad handlar om systemutveckling. Det andra är ett juridiskt fält med fokus på frågor om författningsskydd för den personliga integriteten. Det tredje är ett mer allmänt samhällsvetenskapligt fält som samlar bl.a. informatik, psykologi, marketing och managementforskning. Gemensamt för alla tre fälten är att forskare inom respektive fält endast sällan visar intresse för vad som görs inom något av de andra fälten. Något annat som också framkommit är att det, i forskning som rör personlig integritet, saknas en gemensam begreppsapparat och gemensamma metoder för de olika vetenskapliga fälten och disciplinerna.

Iakttagelserna i översikten kan hjälpa till att förklara varför problemställningar som förekommer inom juridiken (exempelvis att uppgifter hanteras för nya ändamål som är oförenliga med de ursprungliga ändamål för vilka uppgifterna samlades in) inte i högre utsträckning hämtar idéer till lösningar från teknikfältet (exempelvis att uppgifterna anonymiseras på ett sätt som minimerar integritetsriskerna utan att försämra möjligheten att få ny kunskap ur datasamlingen).

[23] Bilaga 3.

3.6 Drivkrafter bakom utvecklingen

Det är viktigt att förstå vilka drivkrafter som ligger bakom utvecklingen för att kunna återkomma till rätt slags åtgärder för att försöka komma till rätta med problemen eller bristerna. En generell drivkraft är t.ex. ambitionen att i så hög grad som möjligt nyttogöra den information man har tillgång till. Vi har sett att den drivkraften ofta leder till att grundläggande principer som att uppgifter ska användas för särskilt angivna ändamål (finalitetsprincipen) och skyldigheten att gallra uppgifter, urholkas. En annan generell drivkraft hos alla aktörer – oavsett om det rör sig om företag eller myndigheter – är att alltid göra uppgifter så användbara som möjligt för så många som möjligt, i syfte att uppnå maximal flexibilitet i den egna organisationen. Vissa integritetskyddande åtgärder, som t.ex. att begränsa den interna åtkomsten till personuppgifter inom organisationen, kan innebära att det blir svårare att snabbt flytta personal mellan olika arbetsuppgifter och därmed påverkas effektiviteten i organisationen. Andra drivkrafter är mer specifika för sina områden. Exempelvis innebär affärsmodellerna för annonsering på nätet respektive för molntjänster, att hanteringen av personuppgifter styrs i en riktning som kan försämra den personliga integriteten.

3.7 Kommitténs bedömning av respektive område

Nedan återges vad kommittén framfört under rubriken *Kommitténs samlade bedömning av området* i kapitel 7–21.

3.7.1 Skolan (kapitel 7)

Av det här kapitlet framgår att det genereras allt fler och allt mer detaljerade uppgifter om eleverna i skolan, alltifrån hur de använder sig av läromedel och chattar med klasskamraterna, till vilka kamrater de helst syns tillsammans med i skolan.

Uppgifterna kan användas på ett sätt som innebär stor nytta för eleverna, t.ex. när de används för att utforma det stöd den enskilde eleven behöver i skolarbetet. Samtidigt finns det ett antal olika risker med den ökande mängden uppgifter om eleverna.

Det mesta av den tilltagande personuppgiftsmassan om eleverna hanteras utan deras eller vårdnadshavarnas samtycke. Det kan också hända att uppgifterna hanteras med stöd av samtycken vars lämplighet eller giltighet kan ifrågasättas.

Det finns oftast tydliga regler om att elever eller vårdnadshavare ska informeras om hanteringen av elevernas uppgifter. Men många gånger har inte ens den ansvarige, dvs. skolhuvudmannen, överblick över vilka uppgifter som hanteras av vem och hur. Den information som sedan ges vidare till elever och vårdnadshavare kan därför ofta antas vara mer eller mindre bristfällig.

De företeelser som nämns i det här kapitlet har inte granskats ur ett integritetsskyddsperspektiv på senare år, förutom när det gäller kameraövervakning och molntjänster. Det finns inte heller någon myndighet eller annan aktör som kan sägas ha en helhetsbild av vad som försiggår med bäring på integritetsskyddet i landets tusentals skolor – i vad mån kameraövervakning används, molntjänster anlitas, vilka sociala medier som används osv.

I sammanhanget är av betydelse att det rör sig om barns rätt till personlig integritet. Barn måste anses som särskilt viktiga när det gäller att skyddas mot otillbörliga intrång i den personliga integriteten, på samma sätt som de anses särskilt skyddsvärda i konsumenträttsliga sammanhang. Barn kan behöva stöd när det gäller att freda sin personliga sfär eller när de behöver fatta beslut som rör deras nutid och framtid.

Ytterligare skäl till att vara särskilt försiktig med en närgången digital kartläggning av barn, är att erfarenheterna från skolan kommer att prägla dem för resten av livet – även när det gäller frågor om vilka intrång som ska accepteras och vad den enskilde kan förvänta sig att få veta och möjlighet att påverka när det gäller den personliga integriteten.

Det talas ibland också om att elever ges ”digitala tatueringar”, som följer dem under hela deras vandring genom utbildningssystemet och kanske även hänger med ut i arbetslivet. Eleverna ges ingen möjlighet att börja om när de byter skola och kanske inte ens när de slutar skolan.[24] Tatueringarna består i personuppgifter och de analyser som gjorts med hjälp av uppgifterna, och som kanske aldrig gallras. Frågan om digitala tatueringar kan antas växa i betydelse i takt med att in-

[24] Se rapporten *Personvern 2015 – tilstand og trender*, från norska Teknologirådet och Datatillsynet, januari 2015.

lärningsanalytiska metoder och arbetssätt vinner terräng och börjar användas av skolorna och systemleverantörerna. Problematiken är snarlik den som brukar anföras i samband med sökmotorernas algoritmer, vilket ibland omtalas som nätets ”filterbubblor” eller ”ekokammare”.[25]

Digitala lärplattformar och digitala läromedel

Det är skolornas huvudmän som är personuppgiftsansvariga för hanteringen av personuppgifter i de digitala lärplattformar och digitala läromedel som används vid skolan, men viktiga beslut som handlar om hantering av elevernas personuppgifter kan många gånger i praktiken fattas av enskilda lärare. Huvudmannen har sällan en fullständig överblick över eller insyn i vilka uppgifter som hanteras i systemen, hur de används och hur länge de sparas. Ibland känner huvudmannen över huvud taget inte till vilka system som används i skolan. Det är kommitténs uppfattning att detta är ett allmänt förekommande problem i skolorna i dag.[26]

Därtill kommer att det för elever i grundskolan och gymnasieskolan inte finns någon sekretess eller tystnadsplikt för större delen av den växande uppgiftsmassan.

En stor andel av undervisningen för landets elever hanteras i digitala lärplattformar och i digitala läromedel. Det rör sig om allt fler och detaljerade uppgifter om varje enskild elev. Dessa uppgifter är av stort intresse för både skolhuvudmän och leverantörer för att dessa ska kunna lära sig mer om eleven, om inlärningsprocesser generellt och om hur plattformar och läromedel fungerar och kan förbättras. Uppgifterna kan därför komma att användas för helt nya ändamål, som eleven och ibland inte heller skolan, känner till och kan påverka. Elevuppgifternas värde innebär också att de kan komma att spridas till exempelvis leverantörernas samarbetsparter. Sekretesskyddet är relativt svagt och det saknas särskild lagstiftning för hanteringen av elevuppgifter, här gäller endast personuppgiftslagen. Sammantaget anser kommittén att användningen av digitala lärplattformar och läromedel innebär en allvarlig risk för den personliga integriteten.

[25] Se kapitel 12 om konsumentområdet.

[26] Denna iakttagelse görs avseende norska förhållanden, som i detta avseende bör vara mycket lika de svenska, se rapporten *Personvern 2015 – tilstand og trender*, från norska Teknologirådet och Datatillsynet, januari 2015.

Samtidigt måste också beaktas att digitala lärplattformar och läromedel kan förbättra undervisningen avsevärt och hjälpa eleverna att uppnå skolans mål.

Sociala medier i undervisningen

Fyra av tio lärare i gymnasieskolan använder sociala medier för att kommunicera med elever. I kommitténs kontakter med skolföreträdare, har uppgetts att det blir allt vanligare att sociala medier används i undervisningen i svenska skolor.

Användningen av sociala medier kan medföra att ett stort antal närgångna uppgifter om den enskilde oavsiktligen exponeras för andra. Vidare förekommer det att sociala medier använder uppgifterna för egna ändamål och sprider dem vidare till andra företag. Det är också svårt för användarna att få klarhet i hur uppgifterna faktiskt hanteras när användarvillkoren väl har godkänts. Den enskildes valmöjlighet är oftast begränsad till att antingen godkänna samtliga villkor, eller att avböja och därmed helt ställa sig utanför det sociala mediet. I avsnittet om sociala medier, bedömer kommittén därför att användningen av vissa sociala medier innebär en allvarlig risk för den personliga integriteten. Risken blir inte mindre vid användning i skolan. Vid sådan användning tillkommer som riskfaktorer att eleverna inte själva får bestämma över det. De blir i stället uppmanade av skolan att använda sociala medier. Skolan bestämmer också hur eleven ska använda sig av det. Det kan bl.a. leda till en oönskad sammanblandning av uppgifter från elevens privata respektive skolrelaterade verksamheter i det sociala mediet.

Samtidigt måste också beaktas att användningen av sociala medier i skolan kan bidra till undervisningen på ett mycket positivt sätt, bl.a. genom att göra det enklare att omvärldsbevaka, kommunicera och dela material med andra elever, lärare och föräldrar.

Elevhälsan

Inom elevhälsan hanteras känsliga uppgifter om alla elever i skolan. Uppgifterna har ett relativt starkt sekretesskydd och elevhälsans hantering av uppgifter omfattas av patientdatalagen. Det saknas undersökningar ur ett integritetsskyddsperspektiv från senare år om

hur personuppgifter från eller inom elevhälsan hanteras i skolorna. Kommittén anser att hanteringen av uppgifter i elevhälsan innebär en viss risk för den personliga integriteten.

Samtidigt måste också beaktas att det är av vikt för elevhälsan, och därmed även för eleverna, att verksamheten kan dra nytta av de fördelar som dokumentation i digitala system kan medföra.

Skolfederationen

Skolfederationen är en tjänst som, använd på rätt sätt, kan innebära att uppgifter ges ett bättre skydd och exponeras för leverantörer i mindre omfattning än vad som annars hade varit fallet. Emellertid är skyddet beroende på skolhuvudmännens och leverantörernas kunskaper och val av inställningar i tjänsten, samt deras medvetenhet om personuppgiftsansvarets placering och innebörd. Mot bakgrund av de bristande kunskaperna om integritetsskydd hos många skolhuvudmän, anser kommittén att Skolfederationen innebär en viss risk för den personliga integriteten.

Kameraövervakning i skolor

Kameraövervakning inomhus förekommer sannolikt i ett betydande antal skolor i dag. Det finns skolor som har ett stort antal kameror inomhus. Det kan därför vara svårt för elever att hitta områden som inte övervakas. Men, det får antas att en så omfattande kameraövervakning inte är vanligt förekommande i landets skolor.

Besluten att införa kameraövervakning delegeras inte sällan långt ner i organisationen och dokumentationen av anledningen till övervakningen är ofta bristfällig. De som övervakas i skolorna tillfrågas sällan om kameraövervakningen och om var och för vilka syften det ska få förekomma. Härtill kommer att teknikutvecklingen har gjort det möjligt att hantera bilderna i exempelvis ansiktsigenkänningsprogram. Kameraövervakning är särskilt reglerad i kameraövervakningslagen. Där regleras bl.a. hur information ska lämnas och hur länge bilderna får lagras. Sammantaget anser kommittén att kameraövervakning inomhus i skolor utgör en påtaglig risk för den personliga integriteten.

Samtidigt måste också beaktas att kameraövervakning inomhus i skolor kan vara ett betydelsefullt verktyg för att uppnå säkerhet och trygghet för eleverna. Det saknas dock svenska undersökningar om detta.

3.7.2 Arbetsliv (kapitel 8)

Ett tydligt och problematiskt fenomen som gäller generellt inom arbetslivet, är risken för ändamålsglidningar när arbetsgivare digitalt hanterar uppgifter om arbetstagare. Det kan också konstateras att Datainspektionens praxis har varit relativt tillåtande inför ändamålsglidningar inom arbetslivet.

Positionering samt annan övervakning av aktiviteter och beteenden

Arbetstagare avsätter allt fler och mer detaljerade elektroniska spår, samtidigt som utrustning och system för att övervaka och kontrollera blir allt billigare och enklare att använda.

En annan del av utvecklingen är att uppgifter om arbetstagare i allt större utsträckning hamnar hos externa leverantörer, inte sällan i molntjänster, som kan innebära en omfattande och svårkontrollerad spridning, lagring och vidareanvändning av uppgifterna. Flera led i den hanteringen görs många gånger utan vare sig arbetsgivarens eller arbetstagarnas kännedom.

Arbetstagaras möjligheter att påverka hanteringen är begränsade redan initialt, pga. arbetsledningsrätten, men försämras ytterligare av bristen på kunskap om hanteringen.

Det sagda, i kombinationen med faran för ändamålsglidningar i arbetslivet, medför att kommittén anser att det finns allvarliga risker för den personliga integriteten när arbetsgivare använder sig av positionering och annan övervakning för att kontrollera arbetstagarnas aktiviteter och beteenden på arbetet.

Samtidigt måste beaktas att arbetsgivaren för att leda, organisera och följa upp arbetet kan behöva relativt detaljerade uppgifter om var arbetstagarna befinner sig, hur de använder sig av arbetsgivarens utrustning och vad de ägnar sin arbetstid åt.

Sociala medier

När arbetsgivare skannar av sociala medier för att bilda sig en uppfattning om vad arbetstagarna gör på nätet, innebär det att arbetsgivaren träder in på en arena som den enskilde vanligen kan betrakta som privat snarare än arbetsrelaterad. Emellertid finns det oftast möjligheter för arbetstagare att begränsa åtkomsten till uttalanden som skulle kunna uppfattas som känsliga eller kontroversiella i förhållande till arbetsgivaren. Därför anser kommittén att arbetsgivares granskningar av vad arbetstagare skriver på sociala medier, innebär en viss risk för den personliga integriteten.

Samtidigt måste anses rimligt att arbetsgivare i sin omvärldsbevakning, inhämtar information från många olika källor, däribland publik information i sociala medier.

Kompetensdatabaser och bakgrundskontroller

Både kompetensdatabaser och utförande av bakgrundskontroller, kan innebära att många olika slags uppgifter om arbetstagarna hanteras. Ibland kan redan enskilda uppgifter vara integritetskänsliga, medan det i andra situationer är sammanställningar av många uppgifter som tillsammans ger en närgången och detaljerad bild av arbetstagaren. Samtidigt är det troligen inte vanligt förekommande med omfattande och detaljerade kompetensdatabaser och bakgrundskontroller. Vidare är spridningen av uppgifterna sannolikt begränsad, liksom många gånger åtkomsten till dem. Kommittén anser därför att kompetensdatabaser och bakgrundskontroller innebär en viss risk för den personliga integriteten.

Samtidigt måste beaktas att arbetsgivare kan behöva dokumentera arbetstagarnas kompetenser och genomföra bakgrundskontroller för att effektivt kunna leda och fördela arbetet och så långt som möjligt undvika felrekryteringar som både kan bli kostsamma och ha negativa effekter för andra arbetstagare hos arbetsgivaren.

Kameraövervakning

Kameraövervakning omfattar allt fler arbetstagare samtidigt som det finns granskningar som visar att många arbetsgivare tillämpar den skyddande lagstiftningen på ett felaktigt sätt. Vidare finns det rapporter om att bilder från kameraövervakning använts för helt andra ändamål än dem för vilka kamerorna installerades. Kommittén anser därför att kameraövervakning på arbetsplatser innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste beaktas att kameraövervakning kan medföra direkta fördelar för enskilda arbetstagare, främst när säkerheten på arbetsplatsen förbättras av kameraövervakningen.

Företagshälsovård

När en vårdgivare ska tillhandahålla både hälso- och sjukvård och personaladministrativa tjänster, kan det uppstå en sammanblandning av vårdgivarens olika roller, som kan få till följd att arbetsgivaren får ta del av uppgifter som hör till hälso- och sjukvårdsdelen av vårdgivarens uppdrag och som omfattas av tystnadsplikt även i förhållande till arbetsgivaren. Det finns emellertid ett tydligt regelverk både för tystnadsplikt gentemot arbetsgivare i dessa situationer, och för hur en vårdgivare får hantera personuppgifter (patientdatalagen). Kommittén anser att det finns en viss risk för den personliga integriteten när vårdgivare ska tillhandahålla såväl hälso- och sjukvård som personaladministrativa tjänster.

Samtidigt kan det finnas fördelar även för den enskilde arbetstagaren om både företagshälsovård och personaladministrativa tjänster tillhandahålls av samma företag, i form av snabbare och enklare kontakt och hjälp vid sjukfall.

Personuppgiftslagen och tillsynen

I kommitténs möten med arbetsmarknadens parter har vidare framkommit att såväl fackliga organisationer som arbetsgivarorganisationer anser att personuppgiftslagen är svår att tillämpa på arbetslivs-

området. Det har också gjorts gällande att Datainspektionens vägledning, i den mån den efterfrågats, inte alltid är tillräckligt tydlig för att ge parterna den hjälp som de behöver.

Brister i kunskap och i den vägledning som ges, kan vara en del av förklaringen till att personuppgiftslagen mycket sällan används som sanktionsmedel av arbetstagarna eller deras organisationer. Det är anmärkningsvärt att det, trots den enorma tekniska utvecklingen, inte har uppkommit särskilt många tvister om personlig integritet inom arbetslivet i samband med användning av informationsteknik.

I likhet med vad som konstaterades i betänkandet *Integritetsskydd i arbetslivet*[27], kan det fortfarande i dag sägas att bestämmelserna i personuppgiftslagen inte förefaller ha fått det genomslag på arbetslivets område som man hade kunnat förvänta sig. I betänkandet kunde vid en internationell jämförelse också konstateras att de finländska och norska motsvarigheterna till personuppgiftslagen haft ett större genomslag på arbetslivets område, utan att några avgörande skillnader finns mellan ländernas dataskyddsrättsliga och arbetsrättsliga lagstiftning. Förklaringen antogs vara att aktiviteten helt enkelt varit högre i dessa grannländer och att man tidigare än i Sverige hade förstått att utnyttja dataskyddsreglerna på arbetslivets område.[28]

Ett särskilt regelverk för integritetsskydd i arbetslivet skulle kunna medföra att det blir lättare för parterna att förstå hur regelverket ska tillämpas på förhållandena i arbetslivet, och därmed kanske skulle kunna leda till att reglerna börjar användas oftare i parternas förhandlingar och tvister.

Kommittén kan också konstatera att Datainspektionens tillsyn görs av enstaka företeelser, men att tillsynen inte leder till att myndigheten får en övergripande uppfattning av hur omfattande övervakningen faktiskt är av landets arbetstagare och i vilka former den bedrivs.

Beträffande kameraövervakning bedömer vi att det inte förefaller troligt att dagens tillsynsinsatser ensamma skulle kunna åstadkomma någon generell förbättring av arbetsgivarnas tillämpning.

Kommittén kan också konstatera att Datainspektionen inte används av parterna i den utsträckning som faktiskt vore möjligt – exempelvis skulle myndighetens bedömning av olika övervaknings-

[27] SOU 2009:44.
[28] SOU 2009:44.

åtgärder kunna inhämtas vid MBL-förhandlingar i samband med införandet av nya system som kan innebära övervakning eller inför tecknandet av nya kollektivavtal.

Sammanfattning

Det är tydligt att ny teknik och nya arbetssätt ökar möjligheterna att kartlägga och övervaka arbetstagare på ett mycket närgånget och detaljerat sätt.

Ny teknik i kombination med nya arbetssätt innebär också risk för en ökande och oönskad sammanblandning av arbetstagarnas privatliv och arbetsliv.

Till detta kommer att den ökande användningen av övervakningstekniker i samhället i stort, träffar arbetstagare även när den egentliga avsikten med övervakningen inte är att kontrollera arbetstagarna, utan verksamhetens kunder, patienter eller brukare. Även när detta görs oavsiktligen, bidrar det ändå till att öka övervakningen av arbetstagarna. Sådan övervakning omfattar särskilt vissa yrken, t.ex. säljare i butik, vårdbiträden samt personal i restauranger och caféer, vilka kännetecknas bl.a. av att de sysselsätter en betydligt högre andel kvinnor än män. Å andra sidan är andra, mer direkt övervakade yrken vanligare för män, t.ex. lastbils- och långtradarförare samt lagerarbetare. Dessa yrken sysselsätter dock färre arbetstagare än i de tidigare nämnda kvinnodominerade yrkesgrupperna.[29]

De ökade möjligheterna till detaljerad kontroll, kartläggning och övervakning i realtid riskerar att förskjuta styrkeförhållandena inom arbetslivet och att försvaga arbetstagarnas ställning.[30]

Samtidigt är det viktigt att beakta att arbetsgivare har en rätt att vidta sådana åtgärder som är rimliga och som faller inom rätten att leda och fördela arbetet. Arbetsgivaren har också en skyldighet att upprätthålla säkerheten för både arbetstagare och utrustning. Effektiva och säkra arbetsplatser har många fördelar även ur den enskilde arbetstagarens perspektiv.

[29] Enligt Statistiska centralbyråns yrkesregister med yrkesstatistik (december 2015).

[30] Norska Datatilsynet uttrycker detta i följande ordalag: ”Den totale mengden av kontrolltiltak og registreringer kan også gjøre at balansen mellom partene i arbeidslivet forskyves ytterligere. Arbeidsgiveren vet mye om hver og enkelt av oss, men vi vet ikke nødvendigvis hva som registreres, hvem som ser hva, og hva opplysningene kan og skal brukes til” Datatilsynets rapport ”*En vanlig dag på jobb” Arbeidshverdagens elektroniske spor*, oktober 2012.

Digitaliseringen i samhället innebär att stora mängder uppgifter om arbetstagare kommer att sparas under oöverskådlig tid och att uppgifterna lätt kan spridas, bearbetas och vara tillgängliga för många. Det är inte förvånande att många arbetsgivare använder sig av olika kontroll- och övervakningsfunktioner för att minska riskerna för felaktiga beslut i verksamheten och vid rekrytering. Samtidigt riskerar denna utveckling att leda till en exkludering från arbetslivet av allt fler individer.

3.7.3 Hälso- och sjukvården och socialtjänsten (kapitel 9)

Hälso- och sjukvård

Tillgången till relevant information är en förutsättning för en god och säker hälso- och sjukvård för alla medborgare. Ett säkert och väl fungerande utbyte av information är en nödvändighet för att medborgarna ska få goda insatser i ett komplext system med många inblandade aktörer. Tillgång till nya informationstjänster har en stor potential att göra patienter långt mer delaktiga i sin vård. Ändamålsenliga och användbara informationssystem är också en förutsättning för att professionerna ska kunna använda sin kompetens och sin tid på det mest effektiva sättet. Funktionella informationssystem är en avgörande faktor för att vården ska kunna hantera framtidens utmaningar.

Kommittén anser att ett gott integritetsskydd också är en nödvändig faktor för att åstadkomma en god och säker hälso- och sjukvård.

Det finns integritetsrisker förknippade med den digitala hanteringen av personuppgifter inom hälso- och sjukvården. Det är nödvändigt att utforma informationsutbytet inom och mellan vårdgivare på ett sådant sätt att det kan göras på ett säkert sätt. Vården måste såväl kunna uppfylla de krav på kvalitet som ställs på de medicinska insatserna som de som ställs på informationshanteringen.

Ökad kunskap, ledning och styrning ifråga om möjligheterna att hantera och utbyta information har stor betydelse för målsättningen att skapa en mer säker, ändamålsenlig och sammanhållen informationshantering inom hälso- och sjukvården. Enligt utredningen om

rätt information i vård och omsorg[31] utgör okunskap om lagstiftningens möjligheter och avsaknad av aktiv rättstillämpning från vårdgivarnas sida en del av problemen med informationshanteringen i hälso- och sjukvården. Detta bekräftas av SLIT-rapporten 2015 som redogör för att det fortfarande återstår anpassning av system, regler och rutiner samt utbildning av personal för att uppfylla patientdatalagens krav.

Kommittén anser att det är anmärkningsvärt att lagen ännu inte implementerats fullt ut och att Datainspektionen flera år efter patientdatalagens ikraftträdande, har hittat allvarliga och systematiska brister även hos stora och resursstarka vårdgivare.

Sammanfattningsvis konstaterar kommittén att risker uppstår i samband med informationshantering inom hälso- och sjukvården till följd av

- bristande ledning och ansvarstagande över informationssystemen och de personuppgifter som hanteras i dessa,
- komplexa miljöer med många olika system för hantering av information,
- brist på gemensamma lösningar, t.ex. gemensam infrastruktur,
- bristande regelefterlevnad,
- bristande kunskaper hos både personal och ledning samt
- bristande informationssäkerhet.

I hälso- och sjukvården hanteras stora mängder känslig information om i stort sett hela befolkningen. Effekten av de brister vid hanteringen som iakttagits kan vara stora för enskilda individer och för hela befolkningen. Flera aktörer uppfyller ännu flera år efter att patientdatalagen trätt i kraft inte de krav på säkerhet som måste ställas vid hantering av känsliga personuppgifter. Mot denna bakgrund bedömer kommittén att det föreligger allvarliga risker för den personliga integriteten i samband med hantering av personuppgifter inom hälso- och sjukvården.

[31] SOU 2014:23, s. 121 och s. 218 i bilaga 4.

Välfärdsteknik och digitala tjänster inom socialtjänsten

Användning av olika digitala och tekniska lösningar i socialtjänsten såsom kameraövervakning, GPS-sändare och sensorer m.m. innefattar hantering av mycket närgångna och känsliga uppgifter om enskilda personer med stort hjälpbehov. Socialtjänsten berör stora delar av befolkningen. Det finns oklarheter i lagstiftningen om på vilket sätt personer med nedsatt beslutsförmåga kan erbjudas tjänster med hjälp av välfärdsteknik. Det finns också risker för bristande informationssäkerhet och bristande ansvarstagande för hur uppgifter hanteras. Kommittén bedömer sammantaget att det föreligger allvarliga risker för den personliga integriteten i samband med hantering av personuppgifter inom socialtjänstens användning av välfärdsteknik.

3.7.4 Forskning och statistik (kapitel 10)

Den övergripande bilden av området är att svenska myndigheter förfogar över ett betydande antal databaser för forsknings- och statistikändamål som tillsammans täcker hela landets totala befolkning. På så sätt utmärker sig Sverige – det finns inte många andra länder som kan jämföra sig med oss när det gäller möjligheten för det allmänna att undersöka sina invånares liv.

Det finns både inom forskningen och inom statistikverksamheten ett stort intresse för att dra nytta av att allt mer data genereras om enskilda och att det samtidigt har blivit möjligt att sammanföra och analysera data från varierande datakällor.

Inom forskningen rör det sig ofta om stora samlingar uppgifter som kan vara synnerligen integritetskänsliga. Inte sällan får uppgifterna hanteras utan information till den enskilde och utan samtycke från denne. Den enskilde har i dessa fall små möjligheter att påverka hur uppgifterna används. De samtycken som inhämtas kan ibland vara mycket breda och endast ge den enskilde en diffus uppfattning om hur uppgifterna faktiskt kan komma att hanteras. Uppgifterna kan också komma att spridas utan den enskildes vetskap. Vidare är det många olika huvudmän med varierande kunskap om integritetsskydd som bedriver forskning. Tillsynen visar också på vissa återkommande brister i hanteringen av personuppgifter inom forskningsprojekt. Sammantaget anser kommittén därför att hantering av integritetskänsliga personuppgifter för forskningsändamål

innebär en allvarlig risk för den personliga integriteten, särskilt när uppgifterna hanteras utan stöd av samtycken eller med stöd av samtycken som är brett formulerade eller som lämnats tidigare i livet.

Även inom den statliga statistikverksamheten rör det sig ofta om stora samlingar uppgifter som kan vara integritetskänsliga. Inte sällan får uppgifterna hanteras utan information till den enskilde och utan samtycke från denne. Den enskilde har i dessa fall inga möjligheter att påverka hur uppgifterna används. Officiell statistik produceras av en rad olika statliga myndigheter, vilka måste kunna skilja mellan hantering av uppgifter i myndighetens kärnverksamhet, och hanteringen inom myndighetens statistikverksamhet. Landets största och känsligaste statistikdatabaser finns emellertid hos två statliga myndigheter: SCB och Socialstyrelsen. Hos dessa två finns tämligen goda förutsättningar att kontrollera hur uppgifterna lagras, lämnas ut och används. Det finns också särskild lagstiftning för den statistikrelaterade hanteringen av personuppgifter hos dessa två och hos övriga statistikansvariga myndigheter. Det saknas tillsynsrapporter som vittnar om brister i samband med statistikverksamhet hos någon statlig myndighet när det gäller integritetsskyddet. Sammantaget anser kommittén att statens hantering av integritetskänsliga personuppgifter för statistikändamål innebär en viss risk för den personliga integriteten.

Samtidigt måste beaktas, beträffande såväl forskning som den statliga statistikverksamheten, att resultaten av dessa verksamheter bidrar med viktiga värden inom en rad olika samhällsområden. Verksamheterna är ur ett samhällsperspektiv mycket viktiga för att kunna planera och utvärdera reformer, för att skapa transparens i samhällsstyret och för att ge bättre underlag för analys, debatt och beslut.

3.7.5 E-förvaltning (kapitel 11)

Digitaliseringen i den offentliga förvaltningen har redan skapat betydande värden i form av bättre service till medborgarna och en effektivare förvaltning. Nyttoeffekten av de olika företeelserna i e-förvaltningen varierar emellertid till art och omfång. Det finns även stora variationer i riskerna för den personliga integriteten som företeelserna innebär.

Inom såväl statlig som kommunal förvaltning hanterar myndigheterna ett stort antal uppgifter om enskilda. Många gånger rör det sig om uppgifter som är känsliga i personuppgiftslagens mening, t.ex. om hälsa, eller som på annat sätt är närgångna och därmed integritetskänsliga, t.ex. uppgifter om enskildas inkomster, sociala problem, skuldsättningar och familjeförhållanden.

Oftast har de enskilda inget inflytande över myndigheternas hantering – den görs i regel utan deras samtycke. Det innebär att det vilar ett särskilt ansvar på det allmänna att se till att uppgifter bara hanteras när det verkligen är nödvändigt för att förvaltningen ska kunna utföra sitt uppdrag och att se till att hanteringen är så säker som möjligt.

Teknikutvecklingen gör det möjligt för den offentliga förvaltningen att utveckla och effektivisera sin hantering av personuppgifter. Det innebär för det första en möjlighet att öka spridningen och vidareanvändningen av uppgifter, dvs. att öka hanteringen rent generellt. Men för det andra innebär utvecklingen också en möjlighet att skydda uppgifterna på ett bättre sätt genom att använda tekniker som stärker den personliga integriteten, t.ex. anonymisering.[32] Dessa två möjligheter går i praktiken ofta att förverkliga samtidigt.

En generell iakttagelse som kommittén gör, är dock att myndigheter och regeringen fokuserar sitt utvecklings- och författningsarbete på den första möjligheten, medan man arbetar betydligt mindre på den andra. Det innebär att offentlig sektor riskerar att bygga in egenskaper i system, arbetsformer och i författningar, som kan bli mycket svåra och dyra att ändra på, om följderna för den personliga integriteten visar sig bli allvarliga.

Informationshantering inom och mellan olika myndigheter

Myndigheterna hanterar i dag fler uppgifter om enskilda än någonsin tidigare. Det finns i dag teknik som gör det enkelt att sprida, vidareanvända och sambearbeta uppgifter, såväl inom en myndighet som myndigheter emellan, eller mellan myndighet och enskilda.

Redan komplexiteten och de tekniska utmaningarna i några av de system som byggts upp för att dela information, kan innebära att utvecklingsresurserna används enbart åt funktionalitet och inte till att analysera frågor som är av betydelse för integritetsskyddet. Det

[32] Se vidare i bilaga 4 om integritetsstärkande tekniker.

förekommer att frågor om t.ex. personuppgiftsansvar, behörighetstilldelning och förenlighet med registerförfattningar behandlas långt senare i utvecklingsprocessen – först när systemet tagits i skarp drift eller inte alls. Anmärkningsvärt är också att det i dessa sammanhang kan finnas brister i viljan hos myndigheter att ta ansvar för både hanteringen av och säkerheten för uppgifter om enskilda personer.

Faktorer som i detta sammanhang är av betydelse för risken för den personliga integriteten, är att det hos vissa myndigheter finns databaser som omfattar hela eller en stor del av befolkningen med uppgifter som kan vara mycket integritetskänsliga. Uppgifter kan spridas till handläggare, inom den egna myndigheten eller på en annan myndighet, som egentligen inte behöver kunna ta del av uppgifterna för att utföra sitt arbete. Enskilda kan i regel inte motsätta sig att deras uppgifter hanteras av myndigheterna. Vi anser därför att den ökade informationsdelningen inom och mellan myndigheter innebär en påtaglig risk för den personliga integriteten.

Samtidigt måste också beaktas att det finns en stor potential för att dessa företeelser både kan användas för att ge bättre service till allmänheten och för att effektivisera förvaltningen.

Informationsutbyte med enskilda

När det gäller e-tjänster som direkt vänder sig till enskilda, exempelvis s.k. egna utrymmen hos myndigheterna, anser kommittén att det finns en viss risk för den personliga integriteten. Faktorer som här är av betydelse för risken för den personliga integriteten, består främst i oklarheter kring personuppgiftsansvaret och i att e-tjänsterna kan ges en teknisk utformning som inte ger ett tillräckligt gott skydd för uppgifterna. Uppgifter kan spridas av misstag eller efter ett antagonistiskt angrepp (hacker-attack) riktat mot myndigheten.

Samtidigt måste också beaktas att det finns en tydlig potential för att sådana tjänster kan vara till stor och direkt nytta för enskilda personer.

Emellertid har vi noterat att myndigheter när det gäller vissa företeelser har en benägenhet att lägga över personuppgiftsansvaret på den enskilde. Det gäller till exempel möjligheten att använda smstjänster eller e-post i kontakten med en myndighet. Det innebär att myndigheten inte fullt ut tar ansvar för att uppgifterna hanteras bara

för de avsedda ändamålen och på ett tillräckligt säkert sätt. Den enskilde förväntas ta ansvar för en hantering som de flesta inte förmår överblicka i sin helhet. När sådana försök till förskjutning av ansvaret förekommer, kan det enligt kommitténs mening medföra att risken potentiellt ökar för den personliga integriteten.

Myndigheter med uppgifter i molnet och bristen på beställarkompetens

Vi har i avsnitt 21.1 om molntjänster gått igenom både risker och fördelar med användningen av molntjänster generellt. Dessa gäller i högsta grad även för myndigheter. Faktorer som för myndigheter är av särskild betydelse för risken för den personliga integriteten, är att myndigheterna kan hantera ett stort antal personuppgifter som kan vara mycket integritetskänsliga, ingå i allmänna handlingar och även omfattas av sekretess. Vidare måste myndigheter veta hur relevanta register- och arkivförfattningar ska tillämpas. Även andra integritetsskyddande regler kan vara av betydelse för myndigheterna, som exempelvis säkerhetsskyddslagen och Myndighetens för samhällsskydd och beredskap föreskrifter om informationssäkerhet hos statliga myndigheter. Många små myndigheter saknar kompetens att välja rätt slags molntjänst som fungerar juridiskt och säkerhetsmässigt för just den aktuella verksamheten. Vi anser att dessa faktorer sammantagna medför att det för myndigheter finns allvarliga risker med molntjänster, i synnerhet i s.k. publika moln (uttrycket förklaras närmare i avsnitt 21.1 om molntjänster).

Samtidigt måste också beaktas att det finns en stor potential för att effektivisera förvaltningen med hjälp av molntjänster, dvs. genom att låta företag lagra och hantera myndigheters data.[33]

Rent generellt för alla slags tjänster inom e-förvaltningen anser vi att det innebär en påtaglig risk för den personliga integriteten, att det alltjämt konstateras stora bister i myndigheters kompetens avseende juridik, informationssäkerhet och kravställning, samtidigt som myndigheterna förväntas börja använda och utveckla nya system och tjänster.

[33] Pensionsmyndigheten utvecklar i en nyligen utgiven rapport de potentiella fördelarna för statliga myndigheter med molntjänster, se *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015.

Myndigheter i sociala medier och med gilla-knappar på webben

Faktorer som i detta sammanhang är av betydelse för risken för den personliga integriteten, är att det finns myndigheter som i förhållande till sociala medier präglas av ett visst mått av naivitet. Myndigheter inser inte alltid att den i onödan kan hjälpa sociala medier, deras samarbetsparter eller företagen bakom sökmotorerna, att kartlägga vad allmänheten gör på nätet. När myndighetens kunskap om detta är begränsad, får besökarna på webbplatsen naturligtvis inte heller tillräckligt med information om att uppgifter om deras aktiviteter på nätet kommer att lämnas ut till företag i tredje land för andra ändamål än att möjliggöra deras besök på myndighetens webbplats. Myndigheternas användning av tjänster från sociala medier och sökmotorföretagen (t.ex. att ha myndighetskonton eller gilla-knappar på den egna webbplatsen), kan innebära att integritetskänsliga personuppgifter lämnas ut till företag i tredje land, även om detta troligen bara görs undantagsvis. Sammanfattningsvis anser vi att myndigheternas användning av tjänster från sociala medier och sökmotorföretagen innebär en viss risk för den personliga integriteten.

Samtidigt är det viktigt att myndigheter kan använda sig av olika media och metoder för att informera brett och effektivt om sina verksamheter, i synnerhet som verksamheterna kan medföra både rättigheter och skyldigheter för den enskilde.

PSI-lagstiftningen

I likhet med PSI-utredningen anser vi att insatserna för att öka spridningen av information från myndigheter till resten av samhället, i kombination med en svårtillämpad och delvis oklar lagstiftning (i första hand PSI-lagstiftningen) innebär en påtaglig risk för den personliga integriteten.

Medborgarprofilering och kontroller på nätet

Av stort intresse för integritetsskyddet är sådan kontrollverksamhet hos myndigheter, som syftar till att i förväg bedöma vilken sannolikhet det finns för att en viss individ ska begå någon form av felaktighet. Av betydelse för risken för den personliga integriteten är att

denna kontrollverksamhet präglas av frånvaro av transparens i förhållande till allmänheten. Detsamma gäller för myndigheters efterforskande verksamhet på öppna eller slutna delar av nätet. Här finns också en rad juridiska, bl.a. grundlagsrelaterade, frågetecken, både avseende de interna kontrollerna och kontrollerna på nätet. Vi anser därför att dessa kontrollverksamheter innebär allvarliga risker för den personliga integritetet.

Samtidigt måste också beaktas att det är synnerligen angeläget, både ur det allmännas och ur medborgarnas perspektiv, att myndigheterna på ett effektivt sätt kan använda sig av egna data och av nätet för att förebygga misstag och oegentligheter.

Informationssäkerhet

De brister i myndigheters informationssäkerhet som vid upprepade tillfällen har konstaterats av flera olika kontrollinstanser, måste sägas medföra en allvarlig risk för den personliga integriteten. Av betydelse i sammanhanget är förstås att myndigheterna hanterar en stor mängd uppgifter som kan vara både känsliga och närgångna och därmed synnerligen skyddsvärda. Brister i informationssäkerheten kan också rent generellt försämra allmänhetens tillit till den offentliga förvaltningen.

Kapitel 22, Informationssäkerhet och integritet, innehåller en redogörelse för informationssäkerhetens betydelse för skyddet av den personliga integriteten.

Brister i regelverket

Brister i regelverket för hantering av personuppgifter inom e-förvaltningen uppmärksammades redan år 2007 av Integritetsskyddskommittén. Kommittén pekade på att det var en genomgående brist att konsekvenserna för den enskildes integritetsskydd inte hade analyserats och beaktats tillräckligt i arbetet, som under senare år har bedrivits för att underlätta myndigheters möjligheter att använda ny teknik och för att främja ett ökat informationsutbyte mellan myndig-

heter. I den mån överväganden av detta slag förekommit, menade kommittén att de inte dokumenterats tillräckligt i förarbetena till lagstiftningen.[34]

Även E-delegationen har i sitt slutbetänkande uppmärksammat att det finns brister i regleringen av förutsättningarna för en effektiv e-förvaltning och ett välavvägt integritetsskydd. E-delegationen bedömer att detta även påverkar enskildas tilltro till myndigheterna, vilket innebär att det är angeläget att regeringen har ett helhetsperspektiv när resultaten av tillsatta utredningar bereds.[35] Även Datainspektionen pekar i sina remissvar regelbundet på brister i nya författningsförslag när det gäller integritetsskyddet.[36]

Vår analys av e-förvaltningen utgår i detta delbetänkande från företeelser som kan ha betydelse för den personliga integriteteten, snarare än från det rättsliga skyddet på området. Emellertid har, som framgår ovan, andra granskningar konstaterat systematiska brister i såväl det befintliga regelverket som i de förslag till nya författningar som framförs på området. Ett genomtänkt regelverk kan bidra till att skydda den personliga integriteten, genom att tydligt peka ut ramar för vad myndigheterna får och ska göra med uppgifterna. Ett sådant regelverk kan också bidra till att myndigheterna känner sig trygga att utveckla nya e-tjänster inom lagstiftningens ramar. Kommittén befarar att bristerna i regelverket för e-förvaltningen kan medföra försämringar i integritetsskyddet.

Datainspektionens roll

Under arbetets gång har flera myndigheter efterlyst tydligare och mer konkret vägledning från Datainspektionen i frågor som rör e-förvaltning och integritetsskydd. Vi avser att återkomma till Datainspektionens uppdrag i slutbetänkandet.

---

[34] Integritetsskyddskommitténs delbetänkande *Skyddet för den personliga integriteten – Kartläggning och analys*, SOU 2007:22.

[35] SOU 2015:66.

[36] Se t.ex. Datainspektionens remissvar den 4 maj 2015 avseende SOU 2015:5, En ny svensk tullagstiftning, myndighetens dnr 404-2015.

Sveriges världsledande roll

I regeringens digitala agenda och e-förvaltningsstrategi sägs att Sverige ska bli världsledande när det gäller digitalisering. Det finns dock inga uttalanden om att skyddet för den personliga integriteten också bör nå en liknande världsledande ställning. En sådan ambition för integritetsskyddet inom e-förvaltningen vore inte orimlig, eftersom det inte alls behöver innebära ett onödigt försvårande av utveckling av nya tjänster som förbättrar servicen till de enskilda och effektiviserar förvaltningen.

Samordning och styrning av utvecklingen

Sammanfattningsvis kan sägas att alla initiativ inom e-förvaltningen – till nya arbetssätt, tillämpning av ny teknik eller ändringar i regelverket – präglas av regeringens höga ambitioner för att påskynda utvecklingen. Samtidigt visar redan kommitténs översiktliga granskning av integritetsrisker inom e-förvaltningen att det på flera punkter finns betydande brister när det gäller både integritetsskydd och informationssäkerhet. Det är också tydligt att det i dag inte finns någon aktör i offentlig sektor som både har övergripande kunskap om vad som händer inom området, och i realiteten utövar en övergripande styrning över e-förvaltningen. Som flera andra, exempelvis E-delegationen och Riksrevisionen, har påpekat, innebär avsaknaden av samordning och styrning en risk för att utvecklingen bromsas och inte uppnår de önskade service- och effektiviseringsnivåerna. Men det innebär också en allvarlig risk för att den personliga integriteten inte skyddas tillräckligt. Risken förstärks av att de satsningar regeringen nu gör för att förstärka samordning och styrning för att utveckla området, inte motsvaras av någon satsning för att förstärka integritetsskyddet inom e-förvaltningen, och inte heller innehåller några direktiv eller tankar kring hur både e-förvaltning och ett gott integritetsskydd ska utvecklas tillsammans i medborgarnas intresse.

3.7.6 Konsumentområdet (kapitel 12)

De senare årens teknikutveckling i kombination med nya användningsområden och nya vanor, har inneburit att det genereras allt mer data om våra konsumtionsrelaterade beteenden.

Det är en allt mindre del av all data i världen som skrivs in eller på annat sätt medvetet genereras direkt av användarna. Mer och mer data genereras i stället rent maskinellt, utan mänsklig inblandning.

Utvecklingen har också inneburit att alla dessa uppgifter i större utsträckning faktiskt går att bearbeta och analysera samlat i realtid.

Den här utvecklingen kan självklart vara till nytta för den enskilde konsumenten på många sätt, men möjliggör samtidigt en allt mer omfattande kartläggning på individnivå. Kartläggningen ökar både på bredden och på djupet genom att fler och nya slags uppgifter samlas in och samkörs.

Ett grundläggande problem är att enskilda användare – trots ett i många delar tydligt regelverk – inte informeras om den ökande hanteringen på ett heltäckande men ändå lättfattligt sätt. Därtill kommer att det rent allmänt finns en relativt låg medvetenhet i befolkningen om hur vardagsgöromål som inte uppfattas som ett uppgiftslämnande, faktiskt genererar elektroniska spår och hur dessa spår samlas in, sparas och används. Det finns inte heller någon större medvetenhet om att personuppgifter faktiskt är en värdefull handelsvara, särskilt i tjänster som marknadsförs som ”gratis”.

Ett annat grundläggande problem är att uppgifter i allt större utsträckning börjar användas för andra ändamål än dem för vilka de ursprungligen samlades in, vilket brukar kallas för ”ändamålsglidning”. Det är inte förenligt med personuppgiftslagen, om det nya ändamålet är oförenligt med det ursprungliga. När ett stort antal i sig harmlösa uppgifter från olika sammanhang bearbetas och analyseras samlat, kan de tillsammans ge nya och tidigare oanade kunskaper om enskildas personligheter och användas för att göra antaganden om deras framtida beteende. Dessa nya kunskaper kan i sin tur väcka intresse för uppgifterna hos aktörer som exempelvis försäkringsbolag och kreditgivare.

Frågan om ändamålet med en hantering är nära förknippad med frågan om de samtycken som enskilda lämnar i olika sammanhang. Det sägs ibland vara den vanligaste lögnen på internet att svara *ja* på frågan om man läst och förstått företagets (dvs. webbplatsens, kund-

klubbens, betalningsföretagets, appleverantörens) användarvillkor och därmed samtyckt till hur ens personuppgifter kommer hanteras.[37] De långa och invecklade användarvillkoren kan vara i stort sett omöjliga att förstå för gemene man, och särskilt för barn eller personer som har en funktionsnedsättning.

En viktig faktor i sammanhanget är de inblandade aktörernas intresse att samla in så mycket data som möjligt om användarna. Det finns i dag en allmänt spridd och mycket stark tro på att även uppgifter som i dagsläget egentligen inte kan användas på något vettigt sätt, i en snar framtid kan förvandlas till avgörande tillgångar, både rent affärsmässigt och för att lösa svåra problem i samhället. Det har uppstått nya affärsmodeller och nya aktörer som har personuppgifter som främsta eller enda handelsvara, som exempelvis datamäklare.

Intresset av att samla in så stora mängder uppgifter som möjligt är således mycket starkt. Det framstår därmed inte som sannolikt att aktörerna eller marknaden på eget initiativ skulle begränsa kartläggningen av konsumenter och ge enskilda reell insyn i hur deras uppgifter hanteras och ge dem möjlighet att påverka hanteringen.

En annan risk för konsumenter avser informationssäkerhet. Som framgått av detta avsnitt är det inte alltid som nya teknikanvändningar möjliggör ett tillräckligt starkt skydd för personuppgifterna.

Det finns emellertid vissa tecken på att allmänheten i samband med Edward Snowdens avslöjanden kan ha blivit något mer medveten när det gäller informationssäkerhetsfrågor och skyddet för de egna personuppgifterna i olika webbtjänster. Avslöjandena har även föranlett många tjänsteleverantörer att förbättra skyddet i sina tjänster genom att exempelvis införa kryptering som bara kunden har nyckeln till.[38]

Men även om det finns enstaka, lovvärda initiativ från aktörerna till att stärka integritetsskyddet för konsumenter, är dessa inte tillräckliga om man betraktar den pågående utvecklingen i sin helhet. Det krävs mer systemövergripande och grundläggande åtgärder för att stärka skyddet – redan i dag och ännu mer i en snar framtid.

---

[37] En studie från år 2008 visade att en genomsnittlig användare skulle behöva 244 timmar för att läsa igenom samtliga användarvillkor för de sajter hon eller han besökte under loppet av ett år. I USA har presidentens vetenskaps- och teknologiråd sammanfattat situationen med att det bara är i en fantasivärld som enskilda faktiskt läser och förstår villkoren och klickar i att de samtycker.

[38] Norska Teknologirådets och Datatilsynets gemensamma rapport *Personvern 2015 – tillstand og trender*, januari 2015.

Det kan också konstateras att flertalet företeelser som nämns i det här kapitlet inte har granskats ur ett integritetsskyddsperspektiv på senare år. De granskningar som görs av Post- och telestyrelsen (kakor) och av Datainspektionen (elektroniska betalningar och WiFi-tracking) är tillsynsaktiviteter riktade mot vissa specifika aktörer.

Konsumentverket omnämner i sin omvärldsrapport för år 2014 digitaliseringens påverkan på konsumenternas ställning, men har därutöver hittills inte varit aktivt när det gäller integritetsskydds-frågor, t.ex. beträffande frågor om de sociala mediernas avtalsvillkor om personuppgifter.[39]

Det finns således i dagsläget ingen myndighet eller organisation som har en uppdaterad och allmän överblick över vilka företeelser som innebär risker för konsumenter, hur spridda företeelserna är, vilka aktörer de används av osv. och som därmed kan sägas ha en överblick över utvecklingen för konsumenters personliga integritet.

En tillkommande risk är att alla uppgifter som genereras av sakernas internet, kan komma att begäras in av olika företag, som exempelvis försäkringsbolag. När de många och detaljerade uppgifterna väl finns, kommer de att attrahera många olika intressenter.

Det är redan i dag mycket svårt att som konsument använda sig av digitaliseringens och teknikutvecklingens alla fördelar utan att, mer eller mindre ofrivilligt, kartläggas på en detaljerad nivå. Det finns en överhängande risk för att det i framtiden kommer att bli ännu svårare.

Bristen på information, samtyckets urholkning, den stora spridningen av uppgifter för nya ändamål och den ökade totala mängden av uppgifter om den enskilde, innebär att kommittén sammantaget anser att det finns allvarliga risker för konsumenters personliga integritet.

Samtidigt måste beaktas att utvecklingen för med sig stora fördelar för den enskilde konsumenten, exempelvis i form av nya tjänster, ökad tillgång till produkter samt större möjlighet till delaktighet och till att själv skapa tjänster och produkter. Utvecklingen visar också vissa tecken på att enskilda blivit mer medvetna och bättre på att tillvarata de möjligheter som faktiskt finns att vidta egna åtgärder för att skydda sin personliga integritet.

[39] Konsumentverkets rapport 2014:13, *Vår omvärld 2014 – rapport till regeringen 2014-11-30*.

3.7.7 Sociala medier och e-post (kapitel 13)

En stor del av landets befolkning, särskilt yngre och kvinnor, använder dagligen sociala medier för att lagra och publicera en mycket stor mängd uppgifter och för att utbyta privat information med andra användare.

Sociala medier kan föra med sig många fördelar för de enskilda användarna, i form av exempelvis nya möjligheter till både kunskap och utbyte med andra. Ur ett integritetsskyddsperspektiv finns det emellertid även en rad risker med användningen av sociala medier.

Användarvillkor är ofta långa och krångligt skrivna. Även i de få fall då användaren faktiskt tagit del av villkoren, är dessa inte sällan så otydliga att många användare inte ens förstår vilka andra användare som kan ta del av uppgifterna han eller hon har publicerat på det sociala mediet, och än mindre för vilka egna ändamål som det sociala mediet kan använda sig av uppgifterna. Användarvillkoren är också ofta vaga när det gäller till vilka samarbetsparter det sociala mediet får sprida uppgifterna och hur dessa får vidareanvändas. Användarvillkoren kan också innehålla oklarheter beträffande hur länge uppgifterna lagras i någon form hos det sociala mediet. Mot den bakgrunden kan det ofta vara mycket svårt för en enskild användare att bilda sig en egen uppfattning om vilka konsekvenser för den personliga integriteten som användningen av det sociala mediet faktiskt innebär.

Särskilt allvarlig är den risken när det gäller unga, som i dag kan vilja lagra och publicera texter och bilder som de senare i livet skulle vilja radera från nätet. De kommer kanske inte att ha den möjligheten, på grund av villkor som en gång har accepterats, eller på grund av att uppgifterna har spridits till tredje parter hos vilka varken användaren eller det sociala mediet har något som helst inflytande.

Ett specialfall av detta är situationen då uppgifter om mycket unga personer lagras eller publiceras av deras föräldrar. När barnen efter hand blir medvetna om hanteringen av uppgifter om dem, kommer det i de flesta fall vara omöjligt för dem att hindra eller ens överblicka spridningen och användningen av uppgifterna.

Förutom att hanteringen är svår att överblicka utifrån användarvillkoren, ger villkoren ofta mycket fria händer åt det sociala mediet att använda sig av uppgifterna för egna ändamål. Särskilt när möjlighet finns att tillföra andra stora mängder uppgifter till uppgifterna

från det sociala mediet och sambearbeta dessa, blir det i praktiken omöjligt för användaren att i förväg veta för vilka ändamål uppgifterna kan komma att användas.

I och med att ny teknik utvecklas kommer alla uppgifter som lagras och publiceras i sociala medier att kunna användas för en allt mer detaljerad och närgången kartläggning bortom användarnas kännedom eller kontroll.

Eftersom sociala medier oftast är baserade på molntjänster som hanterar uppgifterna utanför EES, finns det också en stor risk för att uppgifter om användarna hamnar i länder där lagstiftningen ger ett otillräckligt skydd. Det kan leda till att exempelvis underrättelsetjänster eller andra myndigheter och organisationer utanför EES lagligen kan få åtkomst till uppgifterna för ändamål och på ett sätt som inte hade varit lagligt i Sverige eller i ett annat land inom EES.

Användningen av vissa sociala medier kan medföra att ett stort antal närgångna uppgifter om den enskilde oavsiktligen exponeras för andra användare. Vidare förekommer det att sociala medier använder uppgifterna för egna ändamål och sprider dem vidare till andra företag. Vanligtvis är det också svårt för användarna att få klarhet i vilken hantering som kan förekomma, när användarvillkoren väl har godkänts. Den enskildes valmöjlighet är ofta begränsad till att antingen godkänna samtliga villkor, eller att avböja och därmed helt ställa sig utanför det sociala mediet. Sammantaget anser kommittén att användningen av sociala medier som har de nyss nämnda egenskaperna innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att även sådana sociala medier kan medföra en mycket stor nytta för den enskilde och för samhället i stort, och att många tjänster är mycket populära bland användarna.

En annan risk för den enskildes personliga integritet ligger i vad användare av sociala medier kan skriva och publicera om andra personer. Genom internet och annan elektronisk kommunikation har möjligheterna för enskilda att sprida integritetskränkande uppgifter om andra ökat väsentligt. Nya skyddsintressen har därför uppkommit och medfört ett väsentligt ökat behov av ett bättre utformat straffrättsligt skydd för privatlivet och den personliga integriteten. Med den motiveringen föreslås i betänkandet *Integritet och straff-*

skydd[40] en ny straffbestämmelse om s.k. olaga integritetsintrång som tar sikte på kränkningar som enskilda personer begår mot andra enskilda.

Om oskyddad e-post används för att skicka integritetskänsliga uppgifter, innebär det att uppgifterna kan användas för egna ändamål av de företag som vidarebefordrar meddelandet, även om det görs i strid mot lag. Vidare kan antagonistiska aktörer få åtkomst till uppgifterna genom t.ex. avlyssning. Många organisationer har policyer som ska begränsa möjligheterna att i mejl skicka integritetskänsliga uppgifter om enskilda, men dessa policyer är inte sällan otydliga och dessutom är det svårt att kontrollera hur de följs. Sammantaget bedömer kommittén därför att användning av e-post innebär en påtaglig risk för den personliga integriteten.

3.7.8 Försäkringsverksamhet (kapitel 14)

Numera hanteras en stor del av försäkringsbolagens verksamhet med hjälp av informationsteknik. Den ökade mängden information som finns tillgänglig om enskilda personer ger försäkringsföretagen möjlighet att få bättre underlag för riskbedömning, skadebedömning och för utredning av oklara försäkringsfall. Företeelsen att med hjälp av sensorer mäta rörelse och aktivitet i bilar och hos personer ger möjlighet att göra riskbedömningen säkrare och mer individanpassad. Detta kan vara både en fördel och en nackdel beroende på hur man ser på hur risken ska fördelas i ett större kollektiv.

Den enskildes måste ge sitt samtycke för att ett försäkringsföretag ska få hämta in uppgifter om dennes hälsa från hälso- och sjukvården. Ett samtycke kan dock lämnas utan att den enskilde har tillräcklig insikt om vad samtycket innebär. Försäkringstagaren saknar dessutom i praktiken någon reell möjlighet att vägra lämna samtycke om han eller hon vill ha det aktuella försäkringsskyddet. Om det är oklart vilken ytterligare information som försäkringsföretagen har tillgång till blir det än svårare för den enskilde att förstå konsekvenserna av ett lämnat samtycke.

De nya möjligheterna att genom olika former av digitala egenmätningar lämna underlag för beräkning av försäkringspremier, t.ex. för fordonsförsäkring och personförsäkring ger upphov till nya

[40] SOU 2016:7.

integritetsrisker. Uppgifterna måste hanteras säkert i varje led för att det inte ska uppstå risker för obehörig spridning. Det innebär också ett stort ansvar för bolagen att inte hantera mer känsliga uppgifter än nödvändigt, eftersom tekniken i sig innefattar stora möjligheter till kartläggning av enskilda individers rörelsemönster och livsstil m.m.

När enskilda erbjuds nya möjligheter att få tillgång till uppgifter om sin hälsa genom att t.ex. kunna ta del av sin patientjournal via internet eller genom att samla sådan information på olika hälsokonton uppkommer risker för att tredjepartsintressenter vill ta del av denna information. Försäkringsföretag kan komma att vilja ta del av uppgifter om kundernas hälsa digitalt genom någon form av app knuten till ett hälsokonto, i stället för att få utskrifter ur patientjournalen. En sådan hantering förutsätter höga krav på säkerhet vid överföring av uppgifterna och ställer andra krav på den enskilde när det gäller insikter om vad överföringen av uppgifterna kan få för konsekvenser. Detta ställer i sin tur krav på företagen när det gäller ansvar för hanteringen och för information till kunderna. De risker som hör samman med användning av molntjänster uppstår också i samband med att personuppgifter kommer att behandlas av de företag som erbjuder app-tjänsterna, se vidare avsnittet om molntjänster (21.1).

Av betydelse i detta sammanhang är också att det måste finns ändamålsenliga rutiner som begränsar vilka anställda inom försäkringsföretagen som ska ha tillgång till olika uppgifter om enskilda.

Den stora mängden uppgifter som finns hos försäkringsföretagen representerar ett betydande ekonomiskt värde och skulle kunna samköras med annan information. Det kan därför finnas en risk för handel med uppgifterna. Försäkringsföretagen omfattas inte av några generella regler om tystnadsplikt. Mot denna bakgrund bedömer kommittén att det i dag finns påtagliga risker för den personliga integriteten i samband med försäkringsföretagens verksamhet.

Kommittén anser därtill att det finns särskild anledning att följa försäkringsbranschens framtida inriktning. Förutom den tekniska utvecklingen i stort, i kombination med en tänkbar förändring av branschens policyer och arbetssätt, ser kommittén en utveckling, där helt nya informationskällor uppstår, ibland som en följd av potentiella försäkringstagares egna åtgärder och tillgång till delvis ny information. Den här informationen är många gånger av stort intresse för försäkringsbolagen, samtidigt som den kan vara av mycket käns-

lig natur för den enskilde. Integritetskommittén ser en risk att den här utvecklingen ytterligare rubbar balansen mellan den enskilde försäkringstagaren och dennes försäkringsgivare.

Med tanke på den stora potentiella ökningen av nya informationskällor med känslig information och den tekniska utvecklingen i stort, bedömer kommittén att den framtida hanteringen av personuppgifter inom försäkringsverksamheten kan innefatta allvarliga risker för den personliga integriteten.

3.7.9 Bank- och kreditmarknaden (kapitel 15)

Numera hanteras en stor del av bankernas och kreditmarknadsföretagens verksamhet med hjälp av informationsteknik. Användningen av sådan teknik har också gett dessa företag tillgång till nya typer av uppgifter, som kan användas vid exempelvis kreditprövningar. Detta är på många sätt en positiv utveckling och har bl.a. lett till effektivitetsvinster. Utvecklingen har dessutom medfört en rad förbättringar för kunderna, inte minst när det gäller tillgänglighet. Ett exempel på detta är möjligheterna att använda appar och internetbank för många transaktioner.

Samtidigt gäller de uppgifter som bankerna och kreditmarknadsbolagen behandlar i stor utsträckning enskildas personliga och ekonomiska förhållanden. Sådana uppgifter är normalt att anse som integritetskänsliga. Ett uttryck för detta är att uppgifterna omfattas av tystnadsplikt eller sekretess. Den information om enskilda som finns hos dessa banker och kreditmarknadsbolag ger stora möjligheter att göra en detaljerad kartläggning av en persons liv. Med utgångspunkt från en individs inköpsmönster kan det vara möjligt att dra slutsatser om dennes personlighet. Det har också visat sig att det även i anonymiserade uppgiftssamlingar kan vara lätt att identifiera enskilda individer.

I detta kapitel har vi analyserat risker för integritetsintrång som hör ihop med bankers och kreditmarknadsbolags behandling av personuppgifter i samband med:

– kreditprövning och rådgivning,
– enskildas användning av kreditkort och transaktioner på internet, och
– i samband med rapporteringskrav.

Kreditprövning och rådgivning

Möjligheten att basera kreditprövning på information som normalt inte behandlas hos kreditupplysningsbolagen, exempelvis uppgifter om inköpsmönster, ökar risken för att prövningen blir mindre transparent och för att ovidkommande faktorer beaktas. Om kreditgivare samlar in uppgifter om sina kunder utan att kunderna informeras om vilka uppgifter som behandlas, förlorar den enskilde också möjligheten att kontrollera uppgifterna och att begära rättelse av eventuella felaktiga uppgifter. De s.k. svarta listor som uppges ha förekommit hos en av storbankerna illustrerar detta problem.

Den stora mängden uppgifter som finns hos banker och kreditmarknadsbolag representerar dessutom ett betydande ekonomiskt värde, och kan samköras med annan information. Det finns av dessa skäl en risk för handel med uppgifterna, trots sekretess. Som framgått ovan har det också förekommit att banker har fört vidare uppgifter om kunder som nekats lån.

Av betydelse i detta sammanhang är också att det måste finns ändamålsenliga rutiner som begränsar vilka inom banken eller kreditmarknadsföretaget som ska ha tillgång till olika uppgifter. Huvudregeln bör vara att endast den som behöver uppgifterna i sitt arbete ska ha tillgång till dem. Såvitt framkommit tillämpar banker och kreditgivare allt oftare olika former av åtkomstkontroll inom verksamheten.

I sin kreditgivnings- och rådgivningsverksamhet behandlar banker och kreditgivare en stor mängd uppgifter om en stor del av befolkningen. Uppgifter som sammantaget kan upplevas som närgångna. Det är svårt för en enskild person att veta vilka uppgifter som ligger till grund för en kreditbedömning. Uppgifterna har ett ekonomiskt värde. Kommittén bedömer därför att det föreligger påtagliga risker för den personliga integriteten i samband med kreditprövning och rådgivning.

Kreditkort och transaktioner på internet

När det gäller kreditkort och transaktioner på internet konstaterar kommittén att de digitala spår som skapas genom sådana transaktioner gör det möjligt att kartlägga enskilda personers konsumtionsmönster på ett närgånget sätt. Sådana uppgifter har ett högt kommersiellt värde

och kan komma att användas på sätt som den enskilde inte kan förutse. När det gäller användningen av banktjänster som internetbank och olika appar konstaterar kommittén att det är nödvändigt med hög säkerhet vid sådan behandling på grund av risken för att närgångna uppgifter blir åtkomliga för obehöriga. Digitala banktjänster är också förknippade med risken för den enskilde att bli utsatt för identitetsstölder.

Behandling av personuppgifter i samband med användning av kreditkort och andra transaktioner på internet gör det möjligt att kartlägga enskilda personers konsumtionsmönster. Det handlar om stora mängder uppgifter om i stort sett alla människor. Företeelsen är förknippad med risker för bedrägerier och identitetsstölder. Kommittén bedömer därför att det finns allvarliga risker för integritetsintrång förknippade med användningen av kreditkort och andra digitala transaktioner.

Rapporteringskrav

Det bör vidare understrykas att bankernas och kreditmarknadsbolagen har fått en roll i arbetet mot bl.a. penningtvätt och mot finansiering av terrorism som innebär ett stort avsteg från principen att endast myndigheter får behandla uppgifter om lagöverträdelser som innefattar brott. I arbetet mot sådan brottslighet finns också en risk att helt oskyldiga personer placeras på olika former av sanktionslistor, vilket kan få stora konsekvenser för den enskilde. Den enskilde har i praktiken inte heller någon möjlighet att påverka sådana åtgärder.

Vid spridning av uppgifter till andra länder tillkommer problemet att det i praktiken inte längre går att kontrollera hur uppgifterna används och i övrigt behandlas. De amerikanska myndigheternas behandling av Swift-transaktionerna är ett exempel på detta.

Riskerna i samband med hantering av personuppgifter på grund av olika rapporteringskrav består bl.a. i att uppgiftssamlandet kan påverka helt oskyldiga. Det kan vara svårt att kontrollera uppgifter som lämnats ut internationellt. Men området är reglerat och rimligen drabbas bara ett begränsat antal personer. Kommittén bedömer därför att det finns påtagliga risker för den personliga integriteten i samband med att banker och kreditmarknadsbolag lämnar ut personuppgifter på grund av olika rapporteringskrav.

3.7.10 Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso (kapitel 16)

I detta kapitel har kommittén analyserat integritetsrisker i samband med Kronofogdemyndighetens, kreditupplysningsföretagens och inkassobolagens verksamhet.

Kronofogdemyndigheten behandlar en stor mängd uppgifter om många enskildas personliga och ekonomiska förhållanden. Det är därför nödvändigt att den interna åtkomsten till uppgifterna begränsas på lämpligt sätt. Myndigheten lämnar dagligen ut information om förändringar i utsöknings- och indrivningsdatabaserna samt om gäldenärernas totala skuldsaldo i elektronisk form till kreditupplysningsföretagen. Uppgifterna måste skyddas från en större spridning än vad som är motiverad samt att inte vilka aktörer som helst får tillgång till uppgifterna i digital form. Kronofogdemyndigheten behandlar känsliga uppgifter om gäldenärer, men behandlar inte uppgifter om hela befolkningen. Kommittén har inte fått information om stora brister i myndighetens hantering av personuppgifter. Mot den bakgrunden bedömer kommittén att det finns vissa risker den personliga integriteten i kronofogdemyndighetens verksamhet.

Kreditupplysningsföretagens verksamhet bygger på att de samlar in stora mängder känsliga uppgifter om hela befolkningen som på olika sätt kan ha betydelse vid kreditgivning. Det ligger i sakens natur att det finns en risk att de samlar in fler uppgifter än vad som verkligen är motiverat. Det finns också en risk att vissa insamlade uppgifter inte är korrekta och aktuella samt för att de lagras längre än nödvändigt.

Den enskilde har i vart fall i teorin vissa möjligheter att påverka kreditupplysningsföretagens utlämnande av uppgifter, genom att undvika lån och krediter, men saknar i princip möjlighet att påverka vilka uppgifter som samlas in.

För att minimera riskerna med kreditupplysningsföretagens verksamhet innehåller lagstiftningen olika typer av integritetsskyddande regler. Ett exempel på detta är kravet på att uppgifter som är oriktiga eller missvisande ska rättas, kompletteras eller uteslutas ur registret. Ett annat exempel är kravet på att obehörig tillgång till registren ska motverkas. I detta ligger bl.a. att företagen måste kontrollera att mottagaren har ett legitimt behov av uppgifterna och att utlämnandet görs på ett säkert sätt. Även kravet på att en kreditupplysnings-

kopia ska lämnas till den som upplysningarna avser är viktigt för att minimera risken för integritetsintrång. Tack vare denna kopia får den enskilde bl.a. en möjlighet att kontrollera att de uppgifter som lämnas är korrekta och fullständiga, och att bl.a. kravet på legitimt behov följs.

För närvarande gäller de integritetsskyddande bestämmelserna i kreditupplysningslagen inte vid vissa former av offentliggörande enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Det gäller t.ex. utlämnanden av uppgifter på tekniska upptagningar, t.ex. på usb-minnen. Sådana utlämnanden innebär en avsevärd risk från integritetssynpunkt. Det är angeläget att de integritetsskyddande bestämmelserna görs tillämpliga även på sådana utlämnanden. Mot bakgrund av de ovannämnda riskerna i samband med hantering av känsliga uppgifter om hela befolkningen bedömer kommittén att det föreligger allvarliga risker den personliga integriteten i kreditupplysningsföretagens verksamhet. Kommittén noterar dock att frågan har utretts och för närvarande bereds i regeringskanslitet.

Även *inkassobolag* behandlar stora mängder uppgifter som är känsliga från integritetssynpunkt. De behandlar dock inte uppgifter om lika många personer som kreditupplysningsföretagen. Det finns dock också i sådan verksamhet en risk att behandlingen avser fler uppgifter än nödvändigt, att vissa uppgifter är felaktiga eller inaktuella och, framför allt, att uppgifterna sprids på ett oönskat sätt. I det sistnämnda ligger bl.a. att det måste säkerställas att uppgifterna inte skickas till, eller är åtkomliga för, utomstående. I denna verksamhet är därför personuppgiftslagens krav på säkerhetsåtgärder – och Datainspektionens tillsynsverksamhet – av särskild betydelse.

Kommittén bedömer att det föreligger vissa risker för intrång i den enskildes integritet på grund av behandling av personuppgifter i inkassobolagens verksamhet.

3.7.11 Domstolarnas verksamhet (kapitel 17)

I domstolarna behandlas en stor mängd uppgifter som rör enskildas personliga förhållanden. I många mål- och ärendetyper är det fråga om känsliga personuppgifter. Det ligger dessutom i sakens natur att domstolarna har mycket begränsade möjligheter att själva avgöra vilka personuppgifter som ska behandlas där. Om en part ger in ett

dokument till domstolen, är domstolen – oavsett handlingens innehåll – i regel skyldig att registrera handlingen och kommunicera den med motparten. Även den enskilde har i många fall begränsade möjligheter att påverka vilka personuppgifter som behandlas i domstolen.

Det finns ett starkt intresse av att säkerställa att allmänheten har goda möjligheter till insyn i domstolarnas rättsvårdande och rättsskipande verksamhet. Medborgarna tycks också förvänta sig en enkel tillgänglighet, på samma sätt som när det gäller kontakter med andra aktörer i samhället. Det finns även ett starkt intresse av att domstolarnas verksamhet bedrivs effektivt, så att domar och beslut kan meddelas inom rimlig tid. Allt detta förutsätter bl.a. en ändamålsenlig användning av modern teknik.

I detta kapitel om integritetsrisker som hör ihop med domstolarnas hantering av personuppgifter har kommittén framför allt behandlat riskerna med verksamhetsregister, besöksterminaler, filmade förhör, informationsutbyte med andra myndigheter och utlämnande av uppgifter på medium för automatiserad behandling.

Verksamhetsregister

En risk med domstolarnas verksamhetsregister är att fler uppgifter än nödvändig behandlas i registren och att känsliga personuppgifter behandlas på ett felaktigt sätt. Från och med januari 2016 finns dock en lag som reglerar domstolarnas behandling av personuppgifter. Kommittén bedömer att det finns en viss risk för att behandling av personuppgifter i domstolarnas verksamhetsregister leder till intrång i den personliga integriteten.

Ljud- och bildupptagningar

Risken med ljud- och bildupptagningar i domstol är att känsliga uppgifter sprids till obehöriga. Om en sådan upptagning lämnas ut i strid mot den sekretess som gäller, skulle uppgifterna enkelt kunna spridas på internet. Det finns också risker för att personal som inte är behörig tar del av upptagningarna av nyfikenhet. Det finns dock sekretessbestämmelser som skyddar uppgifterna. I domstolsdatalagen finns bestämmelser om att tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbets-

uppgifter. Kommittén bedömer att det finns en viss risk för intrång i den personliga integriteten i samband med ljud- och bildupptagningar i domstol.

Digitalt informationsutbyte med andra myndigheter

Risken för kränkningar av den personliga integriteten i samband med domstolarnas informationsutbyte med andra myndigheter inom rättsväsendet består i att känsliga uppgifter kan spridas till obehöriga inom eller utanför myndigheterna. Varje deltagande myndighet måste ansvara för sin behandling och upprätthålla rätt säkerhetsnivå. Domstolsdatalagen reglerar under vilka förutsättningar direktåtkomst till domstolens personuppgifter är tillåten. Kommittén bedömer att det finns en viss risk för intrång i den personliga integriteten i samband med detta informationsutbyte.

Utlämnande av uppgifter på medium för automatiserad behandling

Vid utlämnande av uppgifter i elektronisk form, per e-post eller på ett usb-minne finns det en risk för att känsliga personuppgifter kan spridas till obehöriga. Den elektroniska formen innebär större möjligheter för mottagaren att på olika sätt bearbeta uppgifter och sprida informationen än om utlämnande görs på papper.[41] Det kan t.ex. göra det möjligt för enskilda att sammanställa uppgifter till egna belastningsregister. Kommittén bedömer att det föreligger påtagliga risker för intrång i den personliga integriteten i samband med utlämnande av uppgifter på medium för automatiserad behandling.

Skydda integriteten med sekretess

En viktig del i skyddet för den personliga integriteten är möjligheterna att låta sekretess gälla för vissa uppgifter om enskilda. En alltför långtgående offentlighet kan medföra skador på såväl enskilda som allmänna intressen. Intresset av offentlighet i domstol måste exempelvis vägas mot rätten till skydd för privat- och familjeliv enligt artikel 8 i Europakonventionen. En konsekvens av en långtgående

[41] *Domstolsdatalag*, Ds 2013:10 s. 117 f.

offentlighet kan också bli att domstolarna av integritetsskäl låter bli att i sina avgöranden närmare gå in på vissa uppgifter som är av betydelse i målet. Därigenom riskerar en ofullständig bild ges av de skäl som lett domstolen fram till sitt ställningstagande, vilket i sin tur kan ha en negativ inverkan på medborgarnas förtroende för domstolarnas verksamhet.[42]

3.7.12 De brottsbekämpande myndigheternas verksamhet (kapitel 18)

De brottsbekämpande myndigheterna inhämtar information om enskilda på en rad olika sätt och ofta information som är känslig från integritetssynpunkt. Mycket av informationen behandlas därefter bl.a. i olika register. Åtgärderna motiveras av intressen att förebygga, utreda eller beivra brott. Dessa intressen måste anses vara legitima och centrala i en rättsstat. Dessutom syftar brottsbekämpningen i många fall till att skydda just enskildas personliga integritet i olika avseenden.

I detta kapitel om brottsbekämpande verksamhet har kommittén behandlat risker för integritetsintrång i samband med dessa företeelser:

- Hemliga tvångsmedel med stöd av 27 kap. rättegångsbalken (hemlig rumsavlyssning, hemlig kameraövervakning, hemlig avlyssning och övervakning av elektronisk kommunikation samt genomsökning och kopiering av mobiler och datorer).
- Användning av spaningsmetoder som främst regleras av polislagen.
- Polisens aktivitet på internet.
- Behandling av personuppgifter i register.
- Tillgång till uppgifter i flygbolagens register.
- Internationellt informationsutbyte.

[42] Regeringens proposition *med förslag till sekretesslag*, prop. 1979/80:2 Del A, s. 102; se även Ds 2014:33 s. 37 f.

Behovet av, nyttan med och risken för integritetsintrång på grund av olika tvångsmedel har varit föremål för en omfattande kartläggning, framför allt inom ramen för Utredningen om vissa hemliga tvångsmedel.[43] Utredningen gjorde dels en totalundersökning där man inhämtade uppgifter från de brottsbekämpande myndigheterna om varje enskilt ärende där den aktuella lagstiftningen tillämpats, dels djupundersökningar av vissa ärenden. Av kartläggningen framgår bl.a. att det överlag finns ett stort behov av tvångsmedlen samt att vissa tvångsmedel anses vara av särskild nytta, men att det framför allt i utredningar om organiserad brottslighet är av avgörande betydelse att information kan inhämtas på många olika sätt. Samtidigt konstaterades att tvångsmedlen medför integritetsintrång, som dock såväl de brottsbekämpande myndigheterna som domstolarna på olika sätt försökt begränsa vid den praktiska tillämpningen. Det har alltså gjorts en grundlig genomgång där intresset av en effektiv brottsbekämpning har vägts mot intresset av skydd för den enskildes personliga integritet.

Under de senaste åren har det dock mer eller mindre kontinuerligt pågått en rad olika och delvis överlappande lagstiftningsprojekt på området. Så är fallet även i dag. Dessa ständigt pågående förändringar av regelverket gör det svårt att bedöma den samlade effekten av åtgärderna från ett integritetsperspektiv. Samtidigt har vissa lagändringar under senare tid inneburit att regleringen i ökande grad har samlats i 27 kap. rättegångsbalken[44] och därmed gjorts mer överblickbart, vilket får anses vara positivt även ur ett integritetsperspektiv. Vidare har i större utsträckning uppställts krav på beslut från domstol för användning av tvångsmedlen. För dessa ärenden hos domstol har också införts ett ökat krav på offentliga ombud som ska bevaka enskildas integritetsintressen.

Hemliga tvångsmedel med stöd av 27 kap. rättegångsbalken

Tvångsmedlen som utförs med stöd av 27 kap. rättegångsbalken är alltså väl reglerade och innefattar olika skyddsfunktioner för den personliga integriteten. När det gäller hur gällande regelverk följs har dock Säkerhets- och integritetsskyddsnämnden i sin tillsyns-

[43] SOU 2012:44.
[44] Prop. 2011/12:55 och prop. 2013/14:237.

verksamhet uppmärksammat att även om de brottsbekämpande myndigheterna hanterar hemliga tvångsmedel på ett i huvudsak tillfredsställande sätt, föreligger vissa brister i verksamheten. En brist som uppmärksammats är att det material (upptagningar eller uppteckningar) som erhållits genom hemlig tvångsmedelanvändning i vissa fall inte har förstörts tillräckligt snabbt.[45] Det har vidare konstaterats brister bl.a. i myndigheters dokumentation som inneburit att det inte alltid varit möjligt att följa handläggningen av tvångsmedelsärendena samt att hantering av underrättelser till enskilda i flera avseenden varit undermålig.[46]

Kommittén bedömer ur ett riskperspektiv att det föreligger viss risk för den personliga integriteten i samband med användning av olika tvångsmedel med stöd av 27 kap. rättegångsbalken. Vid denna bedömning har kommittén beaktat sannolikheten för att gemene man ska träffas av åtgärden, liksom att företeelserna är väl reglerade och att risken för oönskad spridning är låg.

Ett hemligt tvångsmedel innebär dock ett mycket närgånget intrång i den personliga integriteten för den enskilda person som är föremål för åtgärden.

När det gäller den generella skyldigheten för teleoperatörer att lagra vissa trafikuppgifter gör kommittén bedömningen att denna företeelse utgör ett väsentligt avsteg från den väl etablerade principen att personuppgiftsansvariga bara får lagra personuppgifter som de själva har ett behov av.

Användning av spaningsmetoder som främst regleras av polislagen.

Det finns även ett antal företeelser som är av beaktansvärd betydelse från integritetssynpunkt men som trots detta är mer eller mindre oreglerade i dag, bl.a. användningen av dolda kroppsmikrofoner och handmanövrerade kameror samt möjligheterna att kopiera hela innehållet i datorer och mobiltelefoner. Dessa spaningsmetoder regleras i dag främst av 8 § polislagen. När det gäller dessa företeelser gör

[45] Se t.ex. redovisning den 23 maj 2012 (dnr 97-2012) den 22 maj 2013, dnr 96-2013 respektive den 22 maj 2014 (dnr 891-2014).

[46] Se t.ex. SIN:s uttalanden den 25 mars 2015, dnr 137-2014 och 2088-2014).

kommittén bedömningen att användningen av dessa metoder generellt sett är förknippade med påtaglig risk för intrång i den personliga integriteten.

Polisens spaningsverksamhet på internet och utåtriktade verksamhet i sociala medier

Denna företeelse hör också till ett område med svag reglering.[47] Riskerna handlar t.ex. om bristande insyn över vilka uppgifter som samlas in och behandlas. Kommittén gör bedömningen att dessa företeelser är förknippade med vissa risker för den personliga integriteten.

Behandling av personuppgifter i register

Även när det gäller Polismyndighetens behandling av personuppgifter i register har bl.a. Säkerhets- och integritetsskyddsnämnden uppmärksammat brister. Nuvarande brister förefaller handla om att gällande bestämmelser inte följs snarare än om utformningen av lagstiftningen som sådan. I det avseendet konstaterar kommittén att det finns utrymme för förbättringar. Den stora organisation som Polismyndigheten utgör innebär att en ännu större mängd uppgifter samlas hos en och samma myndighet samt att fler personer kan få tillgång till dessa uppgifter. Det ökar behovet av åtgärder för att säkerställa att uppgifter inte sprids till obehöriga personer i och utanför organisationen. När det gäller polisens behandling av personuppgifter i register bedömer kommittén att företeelsen är förknippade med påtagliga risker för intrång i den personliga integriteten.

Tillgång till uppgifter i flygbolagens register.

Vissa uppgifter från flygbolagen överförs på begäran till de brottsbekämpande myndigheterna. Vidare för Polismyndigheten ett register över passagerare som ankommer direkt från länder som varken ingår i EU eller Schengensamarbetet. Polisen hämtar i viss utsträckning in uppgifter även från EU:s gemensamma system för viseringar. Denna behandling av uppgifter om resenärer är förknippade med risk

[47] Se även kapitel 11 om E-förvaltning.

för att fler uppgifter än nödvändigt samlas in och även med en risk för att de används för andra ändamål än det för vilket de samlades in. Denna risk ökar om uppgifterna inte gallras på ett ändamålsenligt sätt. Det rör sig här om uppgifter om en stor mängd människor som reser och som inte ägnar sig åt brottslig verksamhet. Företeelsen är dessutom internationell. Det finns dock ett skyddande regelverk. Kommittén gör bedömningen att denna företeelse är förknippade med en viss risk för intrång i den personliga integriteten.

Internationellt informationsutbyte

Polisens deltar även i annat internationellt samarbete om utbyte av uppgifter i brottsbekämpande verksamhet. Vid informationsutbyte finns risk för att det leder till en förlorad kontroll över flödet av personuppgifter och att den nationella lagstiftningen inte kan säkerställa ett skydd för informationen. Informationen kan t.ex. komma att användas för andra syften eller få en större spridning än vad som varit avsett. Det kan vidare vara svårt att åstadkomma rättelse och utplåning m.m. avseende uppgifter som har överförts till andra länder. Kommittén bedömer att denna företeelse är förknippad med en viss risk för intrång i den personliga integriteten.

Kommitténs övriga synpunkter

Utöver vikten av intern uppföljning bör också framhållas betydelsen av en effektiv och ändamålsenlig tillsyn. När det gäller den frågan har regeringen tillsatt en särskild utredning – Utredningen om en myndighet med ett samlat ansvar för tillsyn över den personliga integriteten – som har i uppdrag att bl.a. överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet. Uppdraget ska redovisas i september 2016.[48]

Ett annat problem är att myndigheterna i vissa fall inte uppfyller de krav som följer av ny lagstiftning på grund av att det föreligger tekniska problem på it-området. Som exempel på detta kan nämnas att bl.a. 10–11 §§ i gamla polisdatalagen aldrig fick genomslag på

[48] Dir. 2014:164 och dir. 2015:139.

grund av att polisens it-system inte hade de funktioner som krävdes för att kunna uppfylla lagens bestämmelser. Motsvarande reglering finns i 3 kap. 10–13 §§ i nya polisdatalagen. Men dessa bestämmelser behöver inte börja tillämpas förrän den 1 januari 2018.

Avslutningsvis kan konstateras att när det gäller det brottsbekämpande arbetet har den enskilde, av naturliga skäl, begränsade möjligheter att bestämma vilken information som myndigheterna får behandla. Systemet med underrättelse om användningen av hemliga tvångsmedel i efterhand kan i viss mån anses väga upp denna brist. På så sätt får den enskilde åtminstone möjlighet att bedöma vilket integritetsintrång som förekommit och möjlighet att reagera mot sådant som han eller hon anser vara rättsstridigt. Det finns dock undantag från skyldigheten att underrätta den enskilde. I dessa fall finns däremot krav på att det i stället är Säkerhets- och integritetsskyddsnämnden som ska underrättas och som också ska underrättas vid inhämtning av uppgifter om elektronisk kommunikation enligt den s.k. inhämtningslagen. Nämnden ska även på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel eller har varit föremål för polisens personuppgiftsbehandling. Nämnden ska även kontrollera om tvångsmedelsanvändningen och personuppgiftsbehandlingen har genomförts i enlighet med lag eller annan författning. Dessutom finns möjligheten för en registrerad att få ersättning för den skada eller kränkning av den personliga integriteten som en personuppgiftsbehandling i strid med lagen har orsakat.

3.7.13 Försvarsunderrättelseverksamhet och militär säkerhetstjänst (kapitel 19)

Kommittén har i detta kapitel främst behandlat risker för intrång i den personliga integriteten vid behandling av personuppgifter vid signalspaning och vid behandling av personuppgifter i den militära underrättelsetjänstens it-system.

Inhämtningen av uppgifter i försvarsunderrättelseverksamhet och militär säkerhetstjänst syftar till att skydda Sverige och svenska intressen mot yttre hot, vilket är ett angeläget intresse. Säkerställandet av nationella säkerhetsintressen får i sig anses vara ett sådant ändamål som kan motivera inskränkningar av enskildas fri- och rättigheter.

Att landet har en egen säkerhetpolitisk underrättelsesförmåga är också en förutsättning för att vi inte ska vara beroende av andra länders säkerhetsorgan.

Underrättelser hämtas in på en rad olika sätt, men signalspaningen är en av de grundläggande metoderna. Den tekniska utvecklingen på senare tid har inneburit att viktig information som tidigare kunde infångas genom signalspaning i etern, numera i allt högre utsträckning infångas via kabel.[49] Det finns mot den bakgrunden ett starkt intresse av att signalspaning även kan utföras i kabel, särskilt eftersom det saknas alternativa metoder för att uppnå motsvarande resultat.

Försvarsunderrättelsemyndigheterna hanterar dock en mycket stor mängd uppgifter, som många gånger är av privat natur. Det görs dessutom i en verksamhet som omgärdas av stark sekretess vilket innebär mycket begränsade möjligheter till insyn för allmänheten. Myndigheterna har också långtgående befogenheter i sin verksamhet. Detta innebär risker ur ett integritetsperspektiv, men kan i längden även få betydelse när det gäller medborgarnas tilltro till myndigheternas verksamhet. Mycket av den oro som framförts beträffande signalspaning har också handlat om bristande insyn och risken för missbruk.

Den enskilde har av naturliga skäl mycket begränsad insyn i och få möjligheter att påverka om och hur uppgifter behandlas i underrättelseverksamheten. Det finns visserligen en skyldighet för FRA att lämna underrättelser till enskild när det använts sökbegrepp som är direkt hänförliga till en viss fysisk person. Med hänsyn till den sekretess som personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten normalt sett omfattas av, måste dock denna skyldighet anses sakna en praktisk funktion som skydd för enskildas integritet.

När allmänhetens möjligheter till insyn är begränsade, är det desto viktigare med framför allt externa kontrollfunktioner. En viktig sådan funktion när det gäller signalspaningen är till att börja med den tillståndsprövning som görs av en självständig domstol och där en behovs- och proportionalitetsprövning ska göras. I den bedömningen ligger en prövning ur ett integritetsskyddsperspektiv.

[49] I 11:e septemberutredningens betänkande *Vår beredskap efter den 11 september, SOU 2003:32 s. 129*, angavs att 98 procent av trafik till och från Sverige då gick genom kabel, enligt vad FRA upplyst.

Det finns också ett särskilt stort behov av effektiv efterhandsgranskning genom extern tillsyn. Utifrån vad som redovisas i nämnda rapporter och redovisningar från Siun och Datainspektionen framstår det som att de tillämpande myndigheterna tar integritetsfrågan på stort allvar och att följsamheten till gällande regelverk är god, även om vissa brister har uppmärksammats. Riksrevisionen har också bedömt att Siuns granskningsverksamhet i sin tur är effektiv och att försvarsunderrättelsemyndigheterna tar nämndens synpunkter på allvar och genomför åtgärder i enlighet med Siuns beslut.

Vid signalspaning överförs all gränsöverskridande trafik i kabel till vissa samverkanspunkter, men det lagras inga uppgifter vid dessa punkter och endast en begränsad trafikmängd förs vidare till FRA via s.k. signalbärare. Trots detta innebär den verksamhet som bedrivs vid FRA att det i stor utsträckning inhämtas och bearbetas personuppgifter som kan vara av mycket privat och känslig natur. Mot bakgrund av att uppgifterna hämtas in och behandlas av myndigheter som omgärdas av stark sekretess och stora befogenheter skulle kunna göras gällande att riskerna för den personliga integriteten i samband med signalspaning ska bedömas som allvarliga. Intrånget i den personliga integriteten är tveklöst mycket omfattande för de enskilda personer som faktiskt blir föremål för granskning. Mot bakgrund av att det finns tydliga regler om på vilket sätt denna spaning får bedrivas, att kontrollfunktionerna förefaller att fungera och att endast en ytterst liten del av den totala informationen blir granskad, gör kommittén ändå den sammanvägda bedömningen att riskerna inom det här området ska betraktas som påtagliga.

När det gäller behandling av personuppgifter i Must:s it-system handlar det också om behandling av en stor mängd personuppgifter i en verksamhet med liten insyn. Intrånget i den personliga integriteten är tveklöst mycket omfattande för de enskilda personer vars personuppgifter behandlas. Kommittén bedömer dock att det är låg sannolikhet för gemene man att utsättas för denna risk. Kommittén bedömer även att det handlar om en begränsad spridning av de personuppgifter som behandlas. Kommittén bedömer därför att det föreligger en viss risk för intrång i den personliga integriteten i samband med denna typ av personuppgiftsbehandling.

Ovanstående bedömningar bygger på det underlag som kommittén har haft tillgång till.

Avslutningsvis ska nämnas att vissa utländska myndigheter samlar in och bearbetar information om Sverige och om personer som är bosatta i Sverige, på samma sätt som svenska myndigheter gör detta beträffande utländska förhållanden. Denna utländska verksamhet kan även ha andra syften, exempelvis att kartlägga egna medborgare som har flytt till Sverige (s.k. flyktingspionage). De utländska myndigheterna samlar in uppgifter bl.a. genom signalspaning, utan hänsyn till de begränsningar som gäller enligt svensk lagstiftning.

I vissa fall kan sådan utländsk verksamhet upplevas som mer integritetskränkande än om en svensk myndighet skulle ha agerat på motsvarande sätt, exempelvis om den utländska myndigheten arbetar åt en diktatur. I andra fall kan utländska myndigheters behandling av uppgifter upplevas som mindre integritetskränkande än motsvarande nationella behandling, t.ex. på grund av att den enskilde typiskt sätt inte behöver konfronteras med uppgifter som finns hos utländska myndigheter. Oavsett vilket är det uppenbart att även sådan utländsk verksamhet utgör en betydande risk för den personliga integriteten i Sverige. Det är dock svårt för kommittén att närmare bedöma hur och i vilken omfattning sådana intrång förekommer.

3.7.14 Övervakning med kamera (kapitel 20)

Diskussionen om kameraövervakning och personlig integritet är på intet sätt ny. De senaste årens teknikutveckling har dock ändrat förutsättningarna för övervakningen och aktualiserat nya aspekter. Det finns anledning att anta att teknikutvecklingen även har inneburit att kameraövervakningen i samhället har ökat väsentligt. I dagsläget är det dock ingen myndighet som har en samlad bild över hur omfattande kameraövervakningen är. Det finns inte ens någon samlad statistik avseende sådan kameraövervakning som kräver tillstånd eller anmälan. Denna avsaknad av statistik är en brist som gör det svårt att upptäcka förändringar när det gäller användningen av kameraövervakning. Avsaknaden gör det också svårt att bedöma hur omfattande kameraövervakningen faktiskt är.

Redan den omständigheten att kameraövervakning förekommer anses innebära ett intrång i den personliga integriteten, även om övervakningen endast görs i realtid och ingen inspelning förekommer. Om övervakningen spelas in blir intrånget större, beroende

på hur länge materialet bevaras, vilka som har tillgång till det och vad det används till. Om olika kamerasystem kopplas samman med varandra eller om inspelade bilder kopplas samman med information i stora databaser och biometriska funktioner som t.ex. ansiktsigenkänning, möjliggörs en omfattande kartläggning och intrånget i den personliga integriteten kan bli mycket stort. Det ökade antalet kameror, även bland privatpersoner, i kombination med bättre upplösning, billigare lagringsutrymme och möjligheterna till samkörning med uppgifter i andra databaser, innebär stora risker för intrång i den personliga integriteten. Med drönare och kroppsburna kameror är det dessutom större risk än tidigare att man, avsiktligt eller oavsiktligt, filmar känsliga situationer, exempelvis i en trädgård eller ett omklädningsrum. Därtill kommer risken för publicering eller annan otillbörlig spridning av bilder, som ofta innebär ett särskilt stort intrång i den personliga integriteten. När det gäller etablerade former för kameraövervakning finns dock ett skyddande regelverk och en aktiv tillsyn. För närvarande pågår en översyn av kameraövervakningslagen och hur den ska förhålla sig till den nya tekniken. Kommittén gör bedömning att kameraövervakning innebär påtagliga risker för den personliga integriteten.

Kameraövervakningen har övergått från fysiskt avgränsade analoga system till uppkopplade datoriserade installationer. Tekniken utsätts därför för samma typer av risker som alla andra it-system. Det innebär bl.a. att det material som kamerorna överför eller spelar in måste skyddas från intrångsförsök från utsidan och att innehållet måste skyddas från avlyssning när det överförs från kameror till servrarna där materialet lagras. Används s.k. molntjänster uppkommer ytterligare säkerhetsproblem.

Vid lagring av omfattande material ökar också risken för s.k. ändamålsglidning, dvs. för att materialet kommer till annan användning än den för vilken inspelningen ursprungligen gjordes.

Lagring, bildanalys och annan vidareanvändning av bilder och film ökar alltså riskerna som är förknippade med kameraövervakning. Kommittén bedömer därför att lagring och vidarebearbetning av sådana uppgifter är förknippade med allvarliga risker för den personliga integriteten.

Kameraövervakningslagen har till syfte att tillgodose behovet av kameraövervakning, men också att samtidigt skydda enskilda mot otillbörliga intrång i den personliga integriteten. För att åstadkomma

detta skydd innehåller lagen detaljerade bestämmelser om när kameraövervakning är tillåten samt om upplysningsplikt, säkerhet och bevarande av material. Som framgår ovan är det ännu inte helt klarlagt om den regleringen är tillämplig vid användning av vindrutekameror och drönare, vilket i sig är en risk för den personliga integriteten. Det kan även i andra fall vara svårt för en enskild att avgöra om en planerad övervakning omfattas av kameraövervakningslagen, eller om verksamheten anses vara av rent privat natur.[50]

Sammantaget är kameraövervakning ett område där det finns särskild anledning att följa den tekniska utvecklingen, t.ex. i fråga om möjligheter att koppla samman kamerasystem och databaser samt när det gäller risker för otillåten spridning och annat missbruk av material.

3.7.15 Molntjänster (avsnitt 21.1)

Molntjänster har vissa fördelar även ur ett integritetsskyddsperspektiv. Främst genom att säkerheten för personuppgifterna kan vara bättre hos en molntjänstleverantör än i den personuppgiftsansvariges egen it-miljö.

Det förutsätter dock att den personuppgiftsansvariga organisationen har gjort en grundlig risk- och sårbarhetsanalys och ställt krav på säkerheten som motsvarar uppgifternas känslighet. Redan i detta led kan det finnas brister, exempelvis när den personuppgiftsansvarige felaktigt utgår från att det är molntjänstleverantören som ska göra en risk- och sårbarhetsanalys och sedan anpassa säkerhetsåtgärderna därefter. Resultatet kan då exempelvis bli att känsliga hälsouppgifter hanteras över internet med en säkerhet som är anpassad för uppgifter av helt annan, trivial natur. Det innebär i sin tur en risk för att de känsliga uppgifterna läcker ut och blir åtkomliga på internet. En härmed relaterad risk är att den personuppgiftsansvarige kunden gör underförstådda, men felaktiga, antaganden om att tjänsteleverantören genomför olika typer av säkerhetsaktiviteter, som exempelvis regelbundna tester med återläsning av säkerhetskopierad information, penetrationstester och skydd mot skadlig kod.[51]

[50] Jfr EU-domstolens dom den 11 december 2014 i mål nr C-212/13.
[51] Jfr *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015, s. 44.

De största integritetsrelaterade riskerna med molntjänster hänger emellertid ihop med förlusten av insyn och förlusten av kontroll som användningen av molntjänster i regel innebär.

Förlusten av insyn och kontroll innebär att det finns stora risker för att uppgifter kan komma att hanteras för biträdets eller underbiträdets egna ändamål Det finns också en risk för obehörig åtkomst hos leverantörer och underleverantörer. Leverantörer av molntjänster som är gratis eller mycket billiga grundar oftast sin verksamhet på att uppgifterna som hanteras har ett värde i sig. Uppgifterna kan exempelvis användas för att ta fram information om användarna. Efter sambearbetning med andra uppgifter går dessa att använda som annonsunderlag eller för att utveckla nya tjänster. Betalningen för molntjänsten utgörs då i praktiken av det värde som det innebär för leverantören att få åtkomst till uppgifterna. Det innebär att affärsmodellen i sig rymmer en inneboende drivkraft att använda kundernas uppgifter för egna ändamål och att dela med sig av dem till andra företag. I en rapport från år 2012 nämns just molnföretagens affärsmodeller som en av de största utmaningarna för användarnas integritet.[52]

Förlusten av insyn och kontroll innebär också att det finns stora risker för att uppgifterna hamnar hos underleverantörer som är okända för den personuppgiftsansvarige kunden. Det kan innebära att kunden i slutändan inte kan uppfylla sin skyldighet att se till att uppgifterna hanteras för rätt ändamål och på ett tillräckligt säkert sätt. Det finns likaså en risk att uppgifterna hamnar i länder där lagstiftningen ger ett otillräckligt skydd. Det kan exempelvis leda till att myndigheter och andra organisationer utanför EES lagligen kan få åtkomst till uppgifterna för ändamål och på ett sätt som inte hade varit lagligt i Sverige eller i något annat land inom EES.

Risken för detta uppstår så snart molntjänstleverantören är etablerad i ett tredje land, även om uppgifterna rent fysiskt hanteras på servrar i ett EES-land. Det visade sig i juli 2014 när en domstol i USA godkände ett föreläggande för Microsoft från rättsvårdande myndigheter i USA om att lämna ut uppgifter om en persons e-postkonto, utan att behöva begära rättshjälp från myndigheter i Irland.[53] Microsoft uppger sig ha fått liknande propåer från kinesiska myndigheter.

[52] *Privacy in Cloud Computing*, 2012, International Telecommunication Union.

[53] Avgörande den 31 juli 2014 av Chief U.S. District Judge Loretta A. Preska vid United States District Court, Southern District of New York, avgörandet har överklagats.

Många gånger presenteras molntjänster som färdigförpackade lösningar där den potentiella kunden bara har två valmöjligheter: att acceptera standardavtalen eller låta bli att använda tjänsten. Av Datainspektionens praxis framgår att standardavtal för molntjänster ofta ger leverantören goda möjligheter att hantera uppgifter för egna ändamål, även om sådana avtal strider mot 30 § personuppgiftslagen.

Personuppgiftslagen utgår från att det är den personuppgiftansvariga organisationen som bestämmer ändamål och medel för hanteringen av personuppgifter och som ger instruktioner till personuppgiftsbiträdet. Men när personuppgiftsbiträdet är en global molntjänstleverantör, blir förhållandet i praktiken vanligtvis det omvända, dvs. att biträdet bestämmer ändamål och medel som den personuppgiftsanvarige har att rätta sig efter om den vill använda sig av tjänsten.

Det kan vara mycket svårt för små aktörer, exempelvis mindre kommuner, att ha den kunskap som behövs för att bedöma vilka krav som gäller för att det ska vara möjligt att använda sig av en molntjänst på ett lagligt sätt. När kunskapen finns, kan det ändå vara mycket svårt att förmå en global molntjänstleverantör att anpassa sina avtalsvillkor till en liten kommuns krav.

Även om ett avtal med en molntjänstleverantör uppfyller kraven i personuppgiftslagen, är det i praktiken oftast omöjligt för den personuppgiftsanvarige att utöva någon reell kontroll av om uppgifterna verkligen hanteras i enlighet med avtalet.

En annan risk med molntjänster kommer sig av att många av de populäraste tjänsterna är så billiga att det inte krävs någon upphandling eller ens en kontakt med den personuppgiftsansvariga organisationens it-avdelning innan tjänsten börjar användas. Tjänsterna är ofta enkla att använda och kan bidra till att effektivisera arbetet. Anställda kan därför välja att använda tjänsterna utan att organisationens ledning känner till det, eftersom det underlättar arbetsuppgifterna. Ansvaret enligt personuppgiftslagen för hur uppgifterna hanteras kan emellertid inte delegeras, utan ligger kvar på ledningen som helt saknar möjlighet att kontrollera en hantering vars förekomst i organisationen den inte ens känner till.

En komplikation som är specifik för Sverige, är det osäkra rättsläget när det gäller tillämpningen av offentlighets- och sekretesslagen på molntjänster, som uppstått efter det JO-beslut som nämns ovan i avsnittet om det skyddande regelverket.

När det gäller tillsyn var Datainspektionen i en jämförelse med andra EU-länder tidigt ute med att granska molntjänster och har sedan dess varit fortsatt aktiv i tillsynen av molntjänster. Tillsynsverksamheten har av allt att döma resulterat i att de stora molntjänstleverantörerna successivt blivit bättre på att anpassa sina standardavtal till kraven i personuppgiftslagen. Ännu har emellertid ingen hantering granskats som involverar känsliga personuppgifter, såsom molnbaserade journalsystem inom hälso- och sjukvården, försäkringsbranschen eller socialtjänsten.

Ur ett integritetsskyddsperspektiv utmärker sig särskilt publika molntjänster där flera leverantörer är inblandade. Vid användningen av dessa tjänster finns det en stor sannolikhet för att den personuppgiftsansvarige förlorar insyn och kontroll över uppgifterna. Den enskilde vars uppgifter flyttas till molnet har då förstås ännu mindre vetskap om eller möjlighet att påverka hur uppgifterna hanteras. Molntjänstleverantörerna får i praktiken ett större inflytande över hanteringen än den som bär det legala ansvaret gentemot den enskilde. Den personuppgiftsansvarige hamnar inte sällan i ett underläge i förhållande till leverantören, både i fråga om kompetens att bedöma hur tjänsterna fungerar och i fråga om vilka krav som bör ställas på tjänsterna. Publika molntjänster är vanligt förekommande och kan innehålla mycket stora informationsmängder. När en tjänst är gratis eller mycket billig, grundas erbjudandet många gånger på leverantörens vilja och möjlighet att använda uppgifterna i tjänsten för egna ändamål. Sammantaget anser kommittén att publika molntjänster där flera leverantörer är inblandade, innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att molntjänster bidrar till att effektivisera många verksamheter och möjliggöra nya tjänster. Molntjänster kan också ha fördelar ur ett integritetsskyddsperspektiv, främst genom att säkerheten för personuppgifterna kan vara bättre hos en molntjänstleverantör än i den personuppgiftsansvariges egen it-miljö.

3.7.16 Big data (avsnitt 21.2)

Grundtankarna med big data framstår som svårförenliga med de allmänt vedertagna dataskyddsprinciper som kodifierats i dataskyddsdirektivet och som i svensk rätt återfinns i personuppgiftslagen. Frågan är därför i vad mån metoder och affärsmodeller som involverar big data överhuvudtaget kan anses som förenliga med lagstiftning som bygger på dessa dataskyddsprinciper.

Till att börja med bygger big data på en tro på att de flesta datamängder på något sätt kan komma till nytta i framtiden. Det betyder åtminstone på sikt att fler uppgifter kommer att samlas in än vad som noga taget skulle räcka för att tillgodose det egentliga och ursprungliga ändamålet med insamlingen och att dessa uppgifter inte heller kommer att gallras förrän det står helt klart att de inte länge behövs, om ens då. Det kommer sannolikt att leda till att det bildas allt större och detaljerade samlingar av uppgifter om enskilda.

En annan grundläggande tanke med big data är att nya och oväntade samband och förklaringar förväntas uppkomma när tidigare separata uppgiftssamlingar sambearbetas. Det fordrar att uppgifterna hanteras för helt nya ändamål som de enskilda i praktiken varken känner till, kanske inte ens hade kunnat föreställa sig och långt mindre har samtyckt till. Det kan leda till att enskilda fullständigt tappar kontrollen över hur och för vilka ändamål deras uppgifter hanteras.

Sambearbetning av stora mängder uppgifter i olika datasamlingar, som var för sig inte möjliggör identifiering av enskilda, kan leda till att det blir möjligt att identifiera enskilda som finns registrerade bland uppgifterna. På samma sätt blir det också allt svårare att åstadkomma en beständig anonymisering av datasamlingar, eftersom möjligheterna till återidentifiering blir allt bättre.

Vidare kommer ny kunskap om enskilda att uppstå när datasamlingar sambearbetas och okända samband och mönster framträder som har bäring på enskilda. Eftersom det kan röra sig om väldigt stora datamängder, kan resultatet innebära en mycket närgången kartläggning.

En annan risk består i de många möjliga felkällorna i big data. Det som utmärker uppgifterna i dessa sammanhang är volym och variation i typer av uppgifter, men kvalitet (i bemärkelsen riktighet och

aktualitet) är sällan möjlig att upprätthålla eller ens att kontrollera. Det innebär en risk för att det skapas felaktiga uppgifter, och därmed också felaktiga slutsatser, om många personer.

En annan risk är att drivkraften att göra prognoser om enskilda med utgångspunkt i stora mängder historiska data, kan medföra en förstärkning och fördjupning av redan existerande fördomar och leda till diskriminering. Den risken blir ännu allvarligare om prognoserna används till att fatta automatiserade beslut som rör enskildas rättigheter och skyldigheter, utan att någon mänsklig beslutsfattare är inblandad.

Big data har ännu inte varit föremål för någon närmare granskning utifrån ett integritetsskyddsperspektiv i Sverige. Här har dataskyddsmyndigheterna i exempelvis Storbritannien och Norge kommit längre.

Faktorer som i detta sammanhang är av betydelse för risken för den personliga integriteten, är att big data innebär att uppgifter hanteras för nya ändamål som inte är kända vid insamlingen. Det medför att den enskilde förlorar både kännedom om och inflytande över hur uppgifterna hanteras. Med big data blir det särskilt tydligt att personuppgifter betraktas som en handelsvara med ett högt kommersiellt värde. Det medför en avsevärt ökad risk för spridning av uppgifterna till parter som inte är kända för den enskilde.

Kommittén anser därför att big data för med sig en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att big data på ett genomgripande sätt kan komma att effektivisera och förbättra verksamheter i många delar av samhället.

3.7.17 Biometri (avsnitt 21.3)

Användningen av biometriska tekniker innebär flera olika risker för den personliga integriteten. Vissa av de risker som nämns här, behandlas utförligt i Artikel 29-gruppens yttrande från år 2012 om utvecklingen i fråga om biometrisk teknik.[54]

[54] Artikel 29-gruppens yttrande 3/2012 om utvecklingen i fråga om biometrisk teknik, WP 193, antaget den 27 april 2012.

En risk är att biometriska uppgifter behandlas för nya ändamål som är oförenliga med de ändamål för vilka uppgifterna ursprungligen samlades in. Exempelvis kan biometriska uppgifter om gångstil och ansikte användas inte bara för att identifiera enskilda, utan också för att hitta oönskade beteenden eller särskilda behov hos enskilda.

En annan risk är att fler biometriska uppgifter hanteras än vad som behövs för ändamålet, t.ex. att hela fingeravtryck samlas in och lagras när det i själva verket hade varit tillräckligt att bara hantera vissa mätpunkter från fingeravtrycket. Detsamma kan inträffa när uppgifter om DNA inte bara möjliggör identifiering, utan även avslöjar något om den registrerades hälsotillstånd, sjukdomsbenägenhet eller etniska ursprung.

Ytterligare en risk är att biometriska uppgifter inte skyddas tillräckligt och som en följd av detta blir tillgängliga för personer som kan använda uppgifterna för exempelvis identitetsstöld.

Det finns också en risk för att biometriska uppgifter kan användas utan att den enskilde känner till det eller lämnar sitt samtycke, t.ex. vid publicering av bilder på nätet eller i sociala medier där det finns särskild programvara för ansiktsigenkänning.

Det finns slutligen också en risk för överutnyttjande av biometri när tekniken blir billigare, enklare och därmed mer lättillgänglig. Alla sammanhang kräver inte den höga precision som biometri kan erbjuda.

En ökad användning av olika biometriska tekniker i samhället, riskerar att göra det mycket svårt att någonstans i det offentliga rummet kunna vara helt anonym. När kameror och annan utrustning i omvärlden kan läsa av och identifiera den enskildes kropp eller personliga beteende och koppla ihop de biometriska uppgifterna med uppgifter från andra datakällor blir detta avsevärt mycket svårare.

Sammantaget anser kommittén att användningen av tekniker som involverar många och detaljerade biometriska uppgifter, innebär en påtaglig risk för den personliga integriteten.

Samtidigt måste beaktas att biometriska tekniker kan medföra stora fördelar t.ex. genom att bidra till att höja säkerhetsnivån vid åtkomst- eller tillträdeskontroller och genom att göra identifierings- och autentiseringsförfaranden säkrare genom kombination med andra metoder, men också enkla, snabba och bekväma för den enskilde.

4 Overall assessment

In May 2014 the Swedish Government decided to appoint a parliamentary committee to survey and analyse the actual and potential risks of breaches of privacy that may arise in conjunction with the use of information technology in the private and public sector. The Government appointed Göran Gräslund to chair the committee. The Privacy Committee is now submitting its interim report Hur står det till med den personliga integriteten? (What is the privacy situation?) This is a translation of the chapter of the report in which the committee sums up the situation with regard to privacy.

In this section we attempt to assess what the combined impact will be on an individual of all the collection and storage of personal data, surveying and surveillance in which he or she participates or to which he or she is subject in today's increasingly digitised society.

We also examine the general problems that we have identified as encroaching on several areas of society.

In our final report we intend to investigate the steps that could be taken to counteract the risks that we have identified. Here, methods other than legislation may be relevant, such as industry agreements or proactive measures on the part of the supervisory authorities.

4.1 The combined impact on the individual

In Chapter 5, Privacy, we describe how we use the term privacy. In somewhat simplified terms, we understand privacy to mean everything that it would normally seem relevant to safeguard in order for an individual to be assured a reasonable, protected, private sphere. It

is our mission to show, from the perspective of the individual, the combined impact that recent technological and social developments, in all areas, have had on the privacy of individuals.

The development is sometimes termed "the digital revolution", drawing a comparison with the industrial revolution, or "the third industrial revolution", drawing a comparison with mechanisation and the development of steam power, followed by the development of electricity and the combustion engine.[1]

Whatever term or detailed description is chosen, the shift means a comprehensive change to society and the conditions in which individuals live. This trend naturally brings with it a huge potential benefit, but the task of the committee is to focus on actual and potential risks.

Today digital personal data is generated and used to an ever increasing extent in all areas of society. The number of actors is growing, areas of use are increasing, storage times lengthening, more information is being disseminated and exchanged between actors, further processing of data by the respective actors is growing, and dissemination beyond national borders and the ability to process data in real time are on the rise. We are also seeing that some major actors, as a consequence of the development as a whole and their own business strategies, are gaining access to an ever increasing amount of personal data, so giving them the opportunity to draw increasingly complete pictures of individuals.

This trend is due to digitisation and to a gradual change in the way information processing is viewed, both in public administration and in the business sector.

The trend can be described using the following simplified image:

- Previously organisations had one specific purpose for building up a personal data register or a database. Now there is a wide range of purposes.
- Previously data was collected because there was a clear need to do so. Now it is collected because it "might come in useful one day".
- Previously it was important, partly for reasons of cost, to keep storage times low. Now major benefits are seen in retaining data.

[1] Cf. the final report of the Digitalisation Commission, *Digitaliseringens transformerande kraft – vägval för framtiden* (The transformative power of digitisation – choices for the future), SOU 2015:91, p. 68.

- Previously searches and analyses of personal data were done with a particular purpose in mind. Now big data and data mining are a reality.
- Previously personal data was gathered through a specific registration process. Now it happens more or less automatically by an individual taking action and using digital tools.
- Personal data has increasingly become a commodity.

This trend has been made possible despite the fact that basic data protection principles such as duty to inform, obtain consent, erase and what is known as the "purpose principle" continue to apply.

From the point of view of the individual, the trend means that knowledge of how the information will be processed, and the opportunity to influence this, is constantly shrinking in relation to the growth in processing of personal data in society.

Correspondingly, the individual's opportunity to decide, in a truly free choice, how information about him or her is to be handled is also restricted.

The general conclusion of the Privacy Committee is therefore that in a number of areas the individual is suffering a gradual erosion of privacy.

We can see a shift in influence over how the data is handled – from the individual to the personal data controllers and from the personal data controllers to service providers. Service providers often tend to be large, global companies, even though in a formal sense they are only personal data processors and thereby obliged to follow the instructions of the data controllers. The global companies are very big, but few in number and usually based in the United States. This shift therefore also means a concentration and geographical relocation of influence, beyond the jurisdiction of Sweden and the EU.

Regulation of how data may be handled is largely conducted at EU level. National influence from the Government and the Riksdag must thus be exercised through the EU partnership, with the limitations that this involves. On top of this, as stated above, comes the fact that the actual data processing often takes place outside the EU, which in turn reduces the EU's opportunities to influence it. In this context it

is significant that the EU's data protection provisions tend to provide stronger protection than equivalent rules in other parts of the world, such as the United States.

The overall picture of how data is handled today is a challenge to which individuals may react in different ways.

However, it is clear that when knowledge and control are proportionally reduced, the conclusion must be that the situation for privacy is getting worse, irrespective in fact of how one chooses to define the concept of privacy.

The scenario of the individual's declining self-determination in this respect is also a challenge that the state may react to in different ways. It can accept the individual's relatively diminishing awareness and opportunities to exert influence as a given. It may work to increase individuals' awareness and influence. It may also work to prevent such data processing that is not desirable for some reason. The Swedish state has so far chosen a mixture of all three options.

The scenario also raises a question of a different type – are people and their behaviour changed by the accelerating digital processing of their information and their private lives? And if so, how? We commissioned Lund University to produce a systematic review of the literature on digitisation and privacy. It shows that both internationally and in Sweden, there is surprisingly little knowledge of the effect that digital surveillance has on people's behaviour and their view of the world and themselves. There are some studies indicating a risk that a lack of respect for privacy can lead to lower internet usage and lower political engagement (at least online).[2] However, at the moment there is no scientifically valid and empirical evidence that this is the case.

4.2 General problems

Some of the problems are not restricted to any particular part of society but may be encountered by the individual in many different situations. We therefore wish to highlight these and treat them separately.

[2] See the articles listed in the literature review, particularly in the section on the knowledge and behaviour of young people. There are other reports on this too, such as *Global Chilling – The Impact of Mass Surveillance on International Writers*, Results from PEN's International Survey of Writers (January 2015).

4.2.1 Knowledge of how data is handled

One recurring observation is that individuals are largely unaware of and have little knowledge of why and how their personal data is being processed in equipment and services in different contexts. This is confirmed by a number of surveys. For example, in one work-related survey, only 21 per cent of the employees questioned said that they knew what data their employer collected about their internet use.[3] In another survey, 8 out of 10 Swedes questioned considered that they were not in complete control of their data.[4] The committee made a similar observation on companies or agencies that are data controllers. Where these are concerned there are no surveys equivalent to those on the knowledge and attitudes of individuals, but in our contacts with different parties and in our overview of the prevailing situation it has emerged that a lack of knowledge is not uncommon among those responsible either. One clear example of this is agencies that purchase cloud services without looking in more detail into how the data is handled and disseminated within the service.

4.2.2 Opportunity for the individual to exert influence

Several factors make it harder for individuals to influence how their own data is stored and disseminated. This is firstly made more difficult by the growing further processing of data for new purposes in different parts of society, e.g. through big data. Secondly, it is more difficult for people to have control over their own data because we use equipment that generates and disseminates increasing amounts of personal data – through apps and sensors installed in mobile phones and vehicles, for example.

When the individual is unaware of this and is unable to influence how this personal data is handled, the importance of consent is undermined. The consent obtained for different types of data processing increasingly appears to be chimerical. Even in situations where the way in which data is processed is crystal-clear to the individual and clear consent is requested, in practice the individual may often lack a choice because saying no would demand a high price in terms

[3] Report of 26 June 2014 on a survey of its members carried out by the trade union Unionen.
[4] Special Eurobarometer 431, Data Protection, published in June 2015 and the Swedish Data Protection Authority's annual report for 2015, p. 4.

of, e.g. ceasing to consume online media, ceasing to communicate using social networks, being unable to use credit cards and unable to contact certain care providers, for example. Humans are social animals and exist in a technological context that it is very difficult to opt out of in practice. Refusing to consent means being excluded, and is thus rarely a realistic alternative. Consent questions are often worded as binary options, i.e. either the individual consents to everything that the body responsible wants to do with the data in order to provide a particular service or the individual does not consent and cannot therefore use the service at all. There are rarely graduated options. In some contexts, such as public administration, there is also legislation that does not require consent, and the individual has no legal opportunity to oppose their data being handled in this area. This can have far-reaching effects when information from the administrative sphere reaches the private sector, e.g. through cloud services or the principle of public access to official documents.

4.2.3 The individual's own protective measures

The individual's opportunity to take protective measures requires knowledge of how the data is processed and disseminated by companies and agencies, but also knowledge of how information is disseminated by other individuals, e.g. when pictures of individuals are published on social media by other users.

Furthermore, in practice it is often time-consuming and complicated to protect oneself in ways other than non-participation, e.g. by using encrypted e-mail or other technological solutions available to the individual. This does not seem a realistic option for the vast majority. We commissioned a data security specialist to produce an overview of privacy protection technology. The committee shares the assessment made in the report on the opportunities that individuals have available for protecting themselves against breaches of privacy.

> Many day-to-day services that rest on modern information technology and are seen as indispensable, often involve an in-depth survey of the individual. (…) It is hardly possible, as an individual citizen, to defend oneself against the breach of privacy that occurs by using these technologies, other than by actively choosing not to use the majority of them. Few people are likely to consider stopping buying electricity or stopping using a mobile phone, however. The alternative, as a consumer attempting to protect their private

sphere by various means, is often so impractical and expensive that it rarely seems a realistic option other than for those engaged in gross criminal offences. This group of individuals may well take far-reaching steps to avoid leaving an electronic footprint, including solely using cash, always using anonymisation services on the internet and randomly swapping mobile phones and unregistered SIM cards in different places, as well as turning devices off when they are not needed.

4.2.4 What do individuals think?

The fact that individuals – without having any real alternatives – give away their personal data and do not to any major extent take the measures and steps that do nevertheless exist to protect their data, does not mean that individuals in general care nothing for their privacy. In several surveys respondents answer on the contrary that how their data is handled is important to them, that they would like a clear regulatory framework that is upheld and that their trust in different actors varies considerably in this respect. In a major European survey conducted in 2015 on public attitudes to privacy, 52 per cent of the Swedish respondents disagreed with the statement "providing personal information is not a big issue for you".[5]

In another survey, carried out by a trade union, a clear majority of the members questioned answered that they were neither concerned about breaches of privacy at work nor had ever experienced such breaches.[6] When, on the other hand, they were asked to read some examples of surveillance and then state whether they thought the union should push for stronger privacy protection, an equally clear majority thought that the union should do so.

4.2.5 Insufficient supervision

Supervision of how personal data is handled covers only a fraction of all the phenomena that pose a risk in terms of privacy protection. The greatest responsibility for supervision lies with the Swedish Data Protection Authority, whose job has largely remained the same since the agency was founded in 1973. Today the authority has a

[5] Special Eurobarometer 431, Data Protection, published in June 2015 and the Swedish Data Protection Authority's publication *Integritet i fokus* (Privacy in focus), no. 4, 2015.
[6] Report of 26 June 2014 on a survey of its members carried out by the trade union Unionen.

workforce of approximately 45 people, who are also charged with exercising supervision over debt recovery and credit information. The size of the agency and its mandate means that many new phenomena and actors, for obvious reasons, are not examined or assessed at all from a privacy protection point of view, or that this only happens once they have been on the market for a while.

In recent years the situation has been affected by the fact that the Data Protection Authority has gradually cut back its supervisory activities. This is partly explained by a marked increase in the number of reports and documents submitted for consultation by the Government, which has taken resources away from its supervisory operations.[7]

In this area supervision can be said to be particularly important. Firstly, new phenomena arise at a very rapid pace. There is reason to assess many of these from a legal perspective. Secondly, the regulations are relatively imprecise and intentionally general. It is therefore only once the supervisory authority has assessed a new phenomenon that suppliers and users receive any guidance. The result of the supervision can then be used in the outward, proactive work of the supervisory authority to disseminate awareness.

The Swedish Consumer Agency has said that it has experienced certain difficulties exercising supervision in the digital environment. The problems partly concern digital and individually tailored marketing, e.g. on social media, based on more or less detailed profiling. The phenomenon has not been subject to supervision by the Swedish Consumer Agency. Similarly, user conditions for social media have not yet been examined by the Swedish Consumer Agency.

In its survey the committee found that supervision of privacy today is split between several different agencies. Besides the Swedish Data Protection Authority and the Swedish Consumer Agency, supervision in the privacy arena is also carried out by the Swedish Post and Telecom Authority, the Swedish Commission on Security and Integrity Protection, and the county administrative boards. Split supervision can result in a loss of efficiency regarding supervision overall. However, we have refrained from addressing this issue in any greater depth at this time, as it is currently being analysed in *Utredningen om tillsynen över den personliga integriteten* (the Inquiry

[7] Swedish Data Protection Authority annual report for 2015, p. 4.

into supervision of privacy).[8] With the aim of strengthening protection of privacy, the inquiry will consider how more coherent privacy protection could work within a single agency structure by gathering all supervision of the processing of personal data within one agency.

4.2.6 Sanctions

A general issue for the whole area is that the sanction system, both in criminal law and tort law, does not appear to be used to any great extent. Very few cases reach the courts in any case. For example, in the period 2012–2015 we have found only five disputes that came before the district courts in which the case involved damages under the Personal Data Act. The situation in criminal law is no different. In 2014 in Sweden as a whole, a decision was reached in a total of only four cases of breach of the Personal Data Act (by a judicial ruling, imposition of a penalty or decision not to prosecute).

When the system is used at all, it concerns mild punishments and low amounts of damages.

In summary, the sanction system cannot be said to work to its full capacity, as it has not had the effect that was intended when the provisions were introduced.

4.2.7 Globalisation

Another general observation is that digital services are increasingly characterised by globalisation. Many different actors in different countries work together, for example, in providing all the components and programs in a mobile phone. Personal data about the user can sometimes by processed by those who manufactured the phone, the operating system, or the apps it contains. It is not uncommon for the different manufacturers to be located in different continents. The apps in turn are often cloud-based and it is the nature of cloud services that data is moved between different data centres across the world. This also leads to the legislation of these countries being applied to how the data may be handled, which may involve provisions that provide considerably poorer data protection than that in the

[8] Ju 2015:02.

rules in Sweden and the EU, e.g. on the right of the state to access the data. Processing in other countries also means that it is usually impossible in practice to exercise control over and supervise how the data is actually being handled.

Another consequence of globalisation is that agencies need to give out information to companies that are based in other countries, where accordingly it is the other country's laws that regulate how the data may be handled and disseminated further.[9]

4.2.8 Journalistic purposes under the Personal Data Act

One question we do not address in further detail in the examination is that today's Swedish framework legislation, the Personal Data Act, sets out that significant parts of the regulations do not need to be applied in certain situations as this would restrict freedom of expression. Here we are not concerned with publication on the internet using what is known as a voluntary certificate of no legal impediment to publication, which provides protection under the Fundamental Law on Freedom of Expression and thus overrides parts of the Personal Data Act. Publication without a voluntary certificate of no legal impediment to publication also falls outside the remit of the Personal Data Act if publication is for "journalistic purposes". The provision originates in Article 9 of the Data Protection Directive, which contains a corresponding clause. When the provision was tested by the Swedish Supreme Court, the court judged that activities that involve informing, levelling criticism and initiating debate on social issues of importance to the general public must be considered to have a journalistic purpose in the sense of the Personal Data Act. It may also be a journalistic purpose to inform, criticise and debate on certain issues even if this is done in a manner which offends other individuals.[10]

[9] See e.g. Supreme Administrative Court ruling HFD 2014 ref. 66, where the circumstance that a company was based in Norway meant poorer confidentiality protection for data held by the National Board of Health and Welfare in a question of handing over data, because the Norwegian company was not bound by the Personal Data Act.

[10] NJA 2001 p. 409 and Öman & Lindblom, *Personuppgiftslagen* (The Personal Data Act) (15 October 2015, Zeteo), comment on Section 7, paragraph 2 of the Personal Data Act.

In its application the provision has been broadly interpreted and has been applied, for example, to publication online in the form of blogs which contain personal data and which are seen as an infringement of privacy by the people mentioned in them. Because the purpose of publication was judged to be journalistic, publication was not considered to be in breach of the Personal Data Act.[11]

4.2.9 Internet hate

Another significant risk to the privacy of an individual lies in what users of social media may write and publish about other people online.

In recent years an increasing number of different kinds of online hate campaigns have been reported. The phenomenon is often called *internet hate*. For example, the most recent report from the organisation Friends on children's and young people's experience of the internet shows that as many as one in three of those aged 10–16 have been the victim of online harassment in the past year.[12]

In all age groups it is more common for women to face harassment online than men. The Swedish Government report *Integritet och straffskydd*[13] (Privacy and protection provided by criminal law) summarises research into breaches of privacy online. The summary states that there are researchers in the field who consider that many internet hate campaigns have a clear gender aspect in which women are exposed to sexualised harassment to a considerably greater extent than men. According to these researchers, in the long run this can lead to self-censorship, which could be seen as a threat to gender equality and freedom of expression.

Internet hate can also be carried out by organisations. For example, individual journalists have suffered repeated and systematic online harassment from the organisations they are scrutinising, with the clear purpose of forcing this scrutiny to stop.[14]

---

[11] NJA 2001 p. 409.

[12] Friends' internet report 2016.

[13] SOU 2016:7.

[14] In the media, for example, a case in Finland was recently reported; see the article *Grävande journalist blev måltavla för proryska troll* (Investigative journalist targeted by pro-Russian trolls), published on svt.se on 13 March 2016 and written by Ulf Mattmar and Hedvig Eriksson.

The internet is sometimes described as a new arena for threats and harassment. Through the internet and other electronic communication, opportunities for individuals to disseminate information that breaches the privacy of others have increased considerably. New protective interests have therefore arisen, bringing with them a considerably increased need for better designed protection in criminal law for private life and privacy. With this in mind, the report *Integritet och straffskydd*[15] proposes that a new penalty provision for unlawful violation of privacy be introduced in Chapter 4 of the Swedish Penal Code. The proposed provision would mean criminal liability for a person who violates another person's private life by disseminating images or other information in a way that is intended to cause tangible harm to the person who is the subject of the information.

Because internet hate as a phenomenon has thus recently been analysed and as this has also led to a proposal being submitted which seeks to tackle the problem, the committee will refrain from studying the phenomenon in any greater depth.

4.2.10 Principle of public access to official documents

The Freedom of the Press Act of 1766 introduced the principle of public access into Swedish law. It states that all exercising of authority is to be transparent and that anyone who wishes to do so has the right to read the authorities' official documents. Since its introduction the principle of public access to official documents has remained in force virtually continuously, with broad and strong support in the Riksdag. Today the principle is a cornerstone of Swedish democracy.

The principle of public access to official documents takes as its starting point the fact that documents should be public, and that deviation from this may only be made under special circumstances and after the legislator has carefully weighed up the interests of the need for publicity on the one hand and the need for confidentiality on the other, in each individual case.

With the growth of digitalisation new consequences have arisen for the principle of public access. The better and cheaper the technical opportunities for processing data in combination with other data and for disseminating information over the internet become, the

[15] SOU 2016:7.

greater the commercial value of the personal data that government agencies possess. Many companies therefore want to access this data. Some agencies may charge a fee for handing over certain data, whereupon the data gains economic importance for the agency too. Once companies have obtained data with the support of the principle of public access to official documents, they can disseminate and process the information for purposes completely different from those for which the agency originally gathered the data. Sometimes the companies may also publish personally sensitive data on the internet with the protection of the Fundamental Law on Freedom of Expression through a voluntary certificate of no legal impediment to publication, with the consequence that some of the regulatory framework that protects privacy ceases to apply. The issue of the import of voluntary certificates of no legal impediment to publication as regards privacy is currently the subject of an inquiry by the Committee on the Fundamental Laws on the Media.[16]

The Swedish principle of public access to official documents and the European data protection rules can be said to work in principle in different directions – the principle of public access to official documents takes as its starting point publicity (and confidentiality provisions that regulate exceptions), while the main rule of the Data Protection Directive is that personal data must not be disseminated (unless this is supported by any of the provisions of the Directive). The committee judges that the differences in principle have nevertheless been able to be addressed when applying the legislation in practice.

4.2.11 Privacy an important value for the whole of society

Privacy is not merely important for the individual. It is essential for society in general that its population can be free to form opinions and make statements; that they can, fundamentally, spend time doing what they want to do with people they want to spend time with, without outside involvement or interference. The right to privacy (which is a human right enshrined in the Swedish Constitution in its own right) is thus also an important factor for other central and constitutional rights, i.e. for those rights that form the foundation of

[16] Ju 2014:17.

a democratic society, particularly the right to freedom of expression but also the right to freedom of information and freedom to disclose information.

In recent years we have seen several examples of individuals being harassed in order to silence them from creating public opinion, or from engaging in political activity or journalistic scrutiny. If this type of infringement of our fundamental rights has the wider effect of affecting individuals' willingness to communicate their opinion and take part in public debate, this constitutes a threat to democracy.

In the same way, fundamental values can be damaged if individuals refrain from activities due to loss of trust or concern that they will be registered, surveyed or the object of surveillance in a way which could harm them in the longer term.

There is no doubt that in individual cases there are people who have chosen to refrain from exercising their rights after having been the victim of various forms of harassment, threats or pressure. However, the committee has no evidence to definitively determine that the behaviour of the population in general has been affected by increased concern over being attacked on the internet, surveyed or the object of surveillance.

Another rights-related problem is the massive collection of data that enables profiling and individually tailored marketing or individually tailored search results (known as filter bubbles, described in more detail in the section addressing consumers) which can lead to discrimination and exclusion contravening Chapter 1, section 2 of the Instrument of Government, one of the fundamental laws that form the Swedish Constitution.

A further risk involves a potential but far from impossible future scenario in which human rights are no longer upheld in the same way as today, in Sweden or in countries with which we cooperate and to which information flows relatively freely. The major opportunities that exist for agencies and companies to survey individuals might then be used in completely different ways that might be extremely negative for the individual.

4.3 The development of technology

In our examination we have particularly noted certain phenomena of a more technical nature which recur in several areas. These are increasing in use in purely general terms. In our view these are already of vital importance to the protection of privacy but can be expected to have an even greater significance in a not too distant future and may also re-draw the playing field in several ways.

Big data and the internet of things are two such phenomena that we have addressed in the interim report.

Two other phenomena are of an even more technical nature but will move the goalposts for how we will be able to handle personal data in the future: the development of artificial neural networks[17] and the development of the quantum computer.[18]

We have also noted that some other phenomena have not had the impact on privacy that was once predicted. One example of this is RFID tags, which we do mention as a potential risk to privacy, but which a few years ago were expected to have a considerably greater impact on privacy than we judge has actually been the case. This shows that it is hard to predict with any great accuracy which phenomena will have the greatest impact and influence even over a short time frame.

Another observation we have made is that privacy protection technology could be used to a considerably greater extent than is currently the case. Several good examples are addressed in the over-

[17] Sweden's encyclopaedia Nationalencyklopedin explains neural networks as networks of simple additive units that communicate by connections. In biological neural networks the units are nerve cells (neurons) and the links are synaptic connections. Biological neural networks have served as role models for the development of artificial neural networks, which are realised as computer programs, as integrated circuits (neurochips) or with the help of analogue optical technology, e.g. holography. What makes artificial neural networks stand out is partly their ability to learn, the parallelity that results in a high calculation speed and robustness in terms of errors and noise in input data and in the network itself. Examples of areas of application for neural networks include pattern and image recognition, medical forecasts and artificial intelligence.

[18] According to Nationalencyklopedin the major difference between an ordinary computer and a quantum computer is that a string of quantum bits in a quantum computer may be found in a (coherent) superposition of all the quantum bits included in the string, known as parallelism. The quantum bits may also be entangled, which brings very unique opportunities for a quantum computer to carry out calculations. It is these two characteristics, parallelism and especially entanglement, that give a quantum computer its unique properties compared with an ordinary computer. A quantum computer cannot carry out different calculations from an ordinary computer, it can merely perform them in a different way, but it would be able to carry out some calculations much faster than an ordinary computer.

view of privacy protection technology referred to above. The starting point of the overview is that the use of well-designed privacy protection technology makes it possible to achieve a more beneficial equilibrium in weighing up benefits and risks to privacy. In our view this is a clear area for improvement.

Another observation that runs through the entire examination is that the state does not have any overall picture of development in general in this area, either in terms of the development of technology or regarding new working methods that involve processing personal data. According to several reports examining the issue, nor does the state have an overall overview or control over how its own administration is developing in this area, i.e. within government e-administration.

4.4 The knowledge situation

Several general observations are made in the literature review carried out by Lund University referred to above concerning knowledge in the research field of digitalisation and privacy. We believe that their observations are also significant outside the academic environments and reflect general tendencies.

The review shows that research into digitalisation and privacy is relatively strictly divided between three main academic fields. The first is a technical field that is largely about systems development. The second is a legal field focusing on questions of legislative protection for privacy. The third is a more general field in the social sciences which encompasses subjects including informatics, psychology, marketing and management research. What all three fields have in common is that researchers in each respective field only rarely show interest in what is going on in any of the others. Another issue that has also emerged is that in research into privacy there is no shared conceptual apparatus or shared methods for the different scientific fields and disciplines.

The observations in the review may partly help to explain why problems that arise in law (e.g. data being processed for new purposes that are incompatible with the original purposes for which they were gathered) do not to a greater extent draw on the field of technology

in finding solutions (e.g. anonymising data in a way that minimises privacy risks without impairing the ability to gain new knowledge from the data collection).

4.5 Drivers behind development

It is important to understand the drivers that lie behind the development in order to later be able to return to the right kinds of measures to attempt to resolve problems or deficiencies. One general driver is, for example, to make the most use of the information to which one has access. This driver unavoidably leads to fundamental principles such that data must be used for particularly stated purposes (the finality principle) and the obligation to delete data being undermined. Another general driver among all actors – whether this concerns companies or government agencies – is to always make information as usable as possible for as many people as possible, with the aim of achieving maximum flexibility in the organisation concerned. Certain privacy protection measures, such as limiting internal access to personal data in the organisation, can make it more difficult to quickly switch staff between different duties, so affecting the efficiency of the organisation. Other drivers are more specific to their areas. For example, the business models for online advertising and for cloud services respectively mean that the processing of personal data is steered in a direction that may damage privacy.

5 Den personliga integriteten

5.1 Inledning

I kommitténs uppdrag ingår att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet.

Vad som egentligen avses med begreppet personlig integritet är en ständigt återkommande fråga. Någon allmängiltig definition av begreppet finns inte i svensk lagstiftning. Inte heller direktiven innehåller någon definition av vad som avses. Den engelska termen *privacy*[1], som många gånger anses motsvara det svenska begreppet personlig integritet, har beskrivits som ett kameleontliknande ord som används för att ge goodwill åt ett stort antal olika intressen – från sekretess för personuppgifter till reproduktiv autonomi.[2] Judith Jarvis Thomson[3] har till och med gett uttryck för uppfattningen att det mest slående med ”the right to privacy” kanske är att ingen verkar ha en klar bild av vad det är.

Ordet integritet kommer från det latinska ordet *integer* som betyder orörd, hel.[4] I Svenska Akademiens ordlista beskrivs ordet integritet som ”orubbat tillstånd; okränkbarhet; oberoende”. Som anges i direktiven brukar begreppet personlig integritet i vardagligt tal användas för att beteckna individens värde och värdighet.

---

[1] Dock torde termen privacy egentligen ha en något vidare mening än vad som oftast åsyftas med begreppet personlig integritet, och även innefatta personligt oberoende och självständighet (Integritetsskyddskommitténs betänkande *Skyddet för den personliga integriteten*, SOU 2007:22 s. 53).

[2] Lilian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection.*

[3] *The Right to Privacy* ur *Philosofical Dimensions of Privacy: An Anthology.*

[4] Se t.ex. Kommitténs om genetisk integritet betänkande *Genetik, integritet och etik*, SOU 2004:20 s. 106.

Detta kapitel innehåller en beskrivning av ett antal teorier om personlig integritet samt en redogörelse för hur det har tolkats i vissa tidigare lagstiftningsarbeten. Slutligen redovisas hur begreppet används i detta betänkande.

5.2 Teorier om personlig integritet

5.2.1 Inledning

Personlig integritet diskuteras ofta utifrån ett rättighetsperspektiv och utifrån vad som utgör en kränkning av den. Uppfattningen om vad som omfattas av den personliga integriteten har varierat över tid. En vid tolkning utifrån rättighetskatalogen i regeringsformen eller Europakonventionen brukar omfatta rumslig integritet (hemfrid), materiell integritet (egendomsskyddet), kroppslig integritet (skydd för liv och hälsa, mot ingrepp i eller mot kroppen, kroppsvisitation, kroppsbesiktning m.m.), personlig integritet i fysisk mening (personlig frihet och rörelsefrihet) och den personliga integriteten i ideell mening (skyddet för personligheten och för privatlivet inklusive den privata ekonomin). I konsekvens med detta brukar rätten till personlig integritet beskrivas som den enskildes rätt till en privat sfär som är skyddad från fysiska och psykiska intrång.

Många gånger handlar personlig integritet om möjligheten att kontrollera spridning och användning av personlig information. Vilken information som vi vill hålla för oss själva eller dela med andra varierar efter sammanhang. En uppgift som inte är känslig i det sammanhang där den lämnas ut, kan vidare bli känslig t.ex. om den sammanställs med andra uppgifter. Även skälen till att vi vill hålla information för oss själva varierar. Det kan bl.a. handla om vardagliga och sociala behov som att göra skillnad mellan olika relationer och skydda oss från generande situationer, men också i mer utsatta situationer om skydd för t.ex. vår åsiktsfrihet, vår fysiska säkerhet eller rättssäkerhet. Ibland vill vi också begränsa tillgången till information om oss av strategiska skäl, t.ex. i en förhandlingssituation.[5] Vad vi anser höra till vår personliga sfär varierar också mellan individer, och förändras dessutom över tid.

[5] Se vidare Markus Bylund, *Personlig integritet på nätet*, s. 8 f.

Inom filosofin har olika aspekter på syftet med den personliga integriteten behandlats. Från ett libertarianskt perspektiv har ansetts att det är en fråga om individens makt över sitt eget liv och ett begränsande av myndigheters godtyckliga makt, av självförverkligande skäl. Det egalitära perspektivet har däremot framhållit att den personliga friheten även gynnar kollektivet, genom att den möjliggör utövandet av grundläggande rättigheter som yttrande- och organisationsfrihet.[6]

Daniel J. Solove[7] vid George Washington University Law School har delat in olika teoribildningar kring den personliga integriteten i ett antal kategorier. Kategorierna innebär en generalisering och överlappar till viss del varandra, men visar ändå på skillnader i de olika synsätten.

5.2.2 Rätten att bli lämnad i fred

Det första synsättet handlar om rätten att bli lämnad i fred (the right to be let alone). Detta synsätt genomsyrar Samuel D. Warrens och Louis D. Brandels artikel i Harvard Law Review år 1890 med titeln *The Right to Privacy,* vilken torde vara en av de mest kända skrifterna om personlig integritet. Bakgrunden till artikeln var den teknikutveckling som då var aktuell. Tillgängligheten av kameror för privatpersoner, mindre och billigare än tidigare, och tryckpressar hade möjliggjort en ökad spridning av information om enskildas privatliv. Tillsammans med tidningarnas ”affärsmetoder” – på bara några årtionden hade antalet tidningar ökat från 100 som lästes av 800 000 personer till 800 tidningar med 8 000 000 läsare – ledde detta enligt Warren och Brandels till ett ökat behov av skydd för privatlivet och, som det uttrycktes, ”the right to be let alone”. Vad som ansågs omfattas av denna rätt att vara i fred framgick dock mindre klart.[8] Synen på vad som är privat har sedan dess förändrats och dagens tekniska företeelser – t.ex. sakernas internet (Internet of Things), big data, möjligheterna till avlyssning och lagring av trafikdata – innebär helt andra utmaningar.

[6] Bylund, s. 18.
[7] Daniel J. Solove, *Understanding Privacy.*
[8] Se vidare *Understanding privacy s.* 17.

5.2.3 Oönskad tillgång till jaget

Ett annat sätt att se på integritet innebär att individen ska ha möjlighet att värja sig mot oönskad tillgång till ”jaget” (limited access to the self). Sissela Bok har beskrivit detta som ett skydd mot att andra får oönskad åtkomst genom fysiskt tillträde, personlig information, eller uppmärksamhet.[9] Ernest Van Den Haag har uttryckt sig på liknande sätt. Enligt honom är rätten till privatliv en persons exklusiva rätt till en privat sfär där han eller hon har rätt att hindra andra från att titta, utnyttja eller invadera (inkräkta på, eller på annat sätt påverka). Något förenklat kan personlig integritet enligt detta synsätt sägas handla om att begränsa andras tillgång till det som är privat.[10]

Skyddet för den privata sfären har ibland betraktats som något vi har en slags moralisk äganderätt till. Det vi äger får vi hantera som vi vill, så länge vi inte kränker andras motsvarande rätt. Vi kan dock ge upp denna rätt, t.ex. genom att exponera oss för andra i en offentlig miljö.[11]

5.2.4 Hemlig information

I tredje kategorin ryms teorier som går ut på att offentliggörande av information som inte tidigare avslöjats innebär en kränkning av den personliga integriteten (secrecy, the concealment of certain matters from others). Mot detta synsätt har riktats kritik bl.a. på den grunden att vilken information som är känslig, dvs. som vi vill hålla för oss själva, kan variera efter sammanhang och dessutom fylla olika syften. Att vi har delat med oss uppgifter om oss själva till en viss begränsad krets innebär inte nödvändigtvis att vi vill dela den med andra personer.[12]

Bland annat Helen Nissenbaum förespråkar en mer kontextuell syn på integritet, eftersom vad som är känsligt kan variera över tid, i olika situationer och mellan personer.[13] Det har även anförts att den

[9] Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation*, s. 10 f.
[10] Se vidare Solove s. 18 f.
[11] Torbjörn Tännsjö, *Privatliv*, s. 53 f. med hänvisningar.
[12] Se vidare Solove s. 21 f.
[13] *A Contextual Approach to Privacy Online.*

personliga integriteten snarare är en process än något statiskt, där frågan om vad som ska vara publikt eller privat avgörs med utgångspunkt i varje enskild situation.[14]

5.2.5 Kontroll över egna uppgifter och Strömholms kränkningsförteckning

Många teorier om personlig integritet handlar om individens kontroll över uppgifter om henne eller honom (control over personal information – the ability to exercise control over information about oneself).[15] Ett känt exempel är Alan Westin, som tog sin utgångspunkt i den enskildes rätt att kontrollera utflödet av personlig information och som såg utflöde av personlig information som en integritetsförlust. Westin anför bl.a. att ”privacy” är individers, gruppers eller institutioners anspråk på att själva bestämma när, hur, och i vilken utsträckning information om dem kommuniceras till andra.[16] Från detta synsätt på integritet kan paralleller dras till det juridiska krav på samtycke för behandling av personuppgifter, som många gånger uppställs i lagstiftning. Krav på samtycke kan vara ett sätt att ge individen kontroll över hur personuppgifter behandlas.

Alan Westin pekade ut fyra speciella funktioner som ett rättsligt skydd för individens privata sfär bör tillgodose, och som återgavs av Stig Strömholm.[17] Enligt vad som anfördes behövs en ”right to privacy” för känslan av personlig självbestämmanderätt, för att uppnå känslomässig avkoppling, för att kunna genomföra en fri värdering av andras och inte minst eget handlande, och slutligen för att kommunicera fritt med andra efter eget val. Strömholm pekade på olika faktorer som innebär ökade risker för integritetsintrång, däribland de utökade möjligheter till övervakning och behandling av obegränsade informationsmängder som den tekniska utvecklingen inneburit. Som en negativ bestämning av integritetsbegreppet gjorde Strömholm en förteckning över vad han ansåg kunde utgöra integritetskränkningar, vilka i sin tur kan delas in i tre huvudgrupper:

---

[14] Se bl.a. Markus Bylund, a.a., s. 24 f. med hänvisningar.
[15] Solove s. 24 f.
[16] Alan Westin, *Privacy and Freedom*, 1967.
[17] *Individens skyddade personlighetssfär* (ur antologin *Om våra rättigheter; se även SvJT 1971 s. 698 f)*.

1. intrång i en annan persons privata sfär,
2. insamlande av uppgifter om en persons privata förhållanden, och
3. offentliggörande och annat utnyttjande av material om en persons privata förhållanden.

Enligt Strömholm kunde ”privatsfären” eller ”integritetssfären” kränkas genom 14 närmare angivna handlingar.[18] Grovt sammanfattat skulle denna privata sfär vara

> en beteckning för den enskildes intresse av att själv och ensam så att säga reglera dels flödet av den information som utgår beträffande hans förhållanden, dels utnyttjandet av sådan information samt av speciella identifikationsdata (namn, bild, röst).

5.2.6 Det att vara människa

Det finns även en teori enligt vilken den personliga integriteten ses som ett sätt att skydda ”det att vara människa” (personhood).[19] Edward Bloustein har beskrivit det som att det är individualiteten som skyddas, medan Jeffrey Reiman har gett uttryck för uppfattningen att den personliga integriteten skyddar individens intresse av att bli, vara och förbli en person. Stanley Benn betonar att den personliga integriteten handlar om att respektera individens beslut. Även USA:s högsta domstol har framhållit att den personliga integriteten bl.a. innebär att det ska finnas utrymme att själv fatta vissa viktigare beslut.[20]

---

[18] De 14 handlingarna som kan kränka den privata sfären är enligt Strömholm 1) tillträde till och genomsökande av privata lokaler eller annan egendom, 2) kroppsundersökning, 3) medicinska undersökningar, psykologiska tester osv., 4) intrång i en persons privata sfär genom skuggning, spionerande, telefonterror o.d., 5) som ett speciellt kvalificerat eller, genom sina möjliga konsekvenser, speciellt farligt särfall till grupperna 1 och 4, ofredande genom företrädare för massmedierna, t.ex. i form av ”snokreportage”, men även påträngande och brutala intervjuer av olycksoffer, dessas anhöriga eller eljest personer, som har svårt att värja sig, 6) olovlig ljudupptagning, fotografering eller filmupptagning, 7) brytande av brevhemlighet, 8) telefonavlyssning, 9) utnyttjande av elektronisk avlyssningsapparatur, 10) spridande av förtroliga uppgifter (t.ex. genom advokater, läkare, själasörjare), 11) avslöjande inför offentligheten av annans privata förhållanden, 12) olika former av utnyttjande av annans namn, bild eller liknande identifieringsmedel, 13) missbruk av annans ord eller meddelanden (exempelvis genom förvrängda eller helt uppdiktade intervjuer), och 14) angrepp på annans heder och ära.

[19] Översättningen av termen personhood från engelska till svenska, ”det att vara människa”, är hämtad från Nationalencyklopedin.

[20] Se vidare Solove s. 29 f.

5.2.7 Förhållandet mellan människor

En annan teori som har blivit allt populärare brukar kallas ”intimacy”, dvs. intimitet. Enligt den teorin handlar personlig integritet inte bara om individens självförverkligande, utan också förhållandet mellan människor. Robert Gerstein hävdar t.ex. att intima förhållanden inte skulle kunna existera om vi inte höll fast vid att de skulle vara privata.[21]

Irvin Altman har beskrivit samvaron med andra människor som en funktion av personlig integritet. Enligt Altmans synsätt är integriteten en process, snarare än ett tillstånd, där målet är att i varje stund uppnå optimal balans mellan det publika och det privata. Individen behöver ha möjlighet att i varje ögonblick avgöra vad som är privat respektive publikt, eftersom det är något som varierar utifrån förutsättningarna som råder för stunden. Processen bestäms inte bara utifrån individens subjektiva preferenser utan även i samspel med övriga inblandade parter. Synen på personlig integritet som process sätter alltså fokus på att skapa handlingsutrymme för att kontinuerligt reglera vad som är privat respektive publikt. Att på förhand bestämma att en viss sorts personuppgifter ska vara privat eller publikt är ointressant, eftersom det beror på så många olika faktorer i sammanhanget.[22]

5.3 Behandling av begreppet i tidigare lagstiftningsarbeten

5.3.1 Inledning

Det kan konstateras att synen på den personliga integriteten skiljer sig åt, såväl när det gäller vad som omfattas som vilka syften den har. Begreppets innebörd har behandlats i olika lagstiftningssammanhang. Fram till den grundlagsändring som gjordes år 2011 var utvecklingen av integritetsskyddet framför allt inriktad på att förbjuda företeelser som inte ansågs försvarbara efter beaktande av dels den skada de skulle innebära för den personliga integriteten, dels de motstående intressen – t.ex. brottsbekämpning och intresset av offent-

[21] Se vidare Solove s. 34 f.
[22] Se vidare Bylund s. 24 f.

lighet – som funnits att beakta.[23] I detta avsnitt redovisar vi ett antal utredningar som har övervägt innebörden av begreppet personlig integritet ur ett mer generellt perspektiv.

5.3.2 1966 års integritetsskyddskommitté och Yttrandefrihetsutredningen

Bland äldre utredningar kan särskilt nämnas *1966 års integritetsskyddskommitté* som hade i uppdrag att utreda frågor om förstärkt integritetsskydd på personrättens område. Utöver sitt slutbetänkande *Privatlivets fred*[24] lämnade kommittén tre delbetänkanden om skydd mot avlyssning, olovlig fotografering och kameraövervakning samt reklam och integritet. I slutbetänkandet behandlades problem som är förenade med intrång i privatlivet genom användning och spridning av integritetskränkande material. Kommittén lyfte särskilt fram intrång i privatlivet som uppstår genom att uppgifter av privat natur sprids av massmedierna press, radio och TV samt den konflikt som ofta uppstår mellan intresset att skydda den enskildes privatliv å ena sidan, och massmediernas intresse och uppgift att säkerställa ett fritt meningsutbyte och en allsidig upplysning i samhället å andra sidan. Enligt kommittén torde grundtanken med personlig integritet kunna uttryckas så, att den enskilde kan göra anspråk på en fredad privat sektor inom vilken han kan avvisa inblandning från utomstående. Integritetsbegreppet ansågs i det sammanhanget vara liktydigt med den enskildes anspråk på att information om hans privata angelägenheter inte ska vara tillgänglig för eller få begagnas av utomstående utan hans vilja.[25]

Slutbetänkandet lämnades vidare till Yttrandefrihetsutredningen för att beaktas i denna kommittés arbete. I deras betänkande[26] behandlades bl.a. frågan om kriminalisering av kränkningar av privatlivets fred. Kommitténs bedömning var att en sådan kriminalisering inte borde införas och framhöll att hänsynen till den personliga integriteten hade fått stort utrymme i olika lagstiftningssammanhang, bl.a. den dåvarande sekretesslagen (1980:100).

[23] SOU 2007:22 s. 52.
[24] 1966 års integritetsskyddskommittés slutbetänkande *Privatlivets fred*, SOU 1980:8.
[25] SOU 1980:8 s. 9.
[26] Yttrandefrihetsutredningens betänkande *Värna yttrandefriheten*, SOU 1983:70.

5.3.3 Data- och offentlighetskommittén

Data- och offentlighetskommittén hade i uppdrag att utreda bl.a. användningen av personnummer inom den offentliga och den enskilda sektorn samt problem som var förenade med offentlighetsprincipens tillämpning på upptagningar för automatisk databehandling. I delbetänkandet[27] föreslog kommittén bl.a. att ett skydd för den enskildes personliga integritet i datasammanhang skulle skrivas in i regeringsformens fri- och rättighetskatalog, vilket senare också gjordes. Kommittén framhöll att det rests krav på ett stärkt skydd mot intrång i medborgarnas personliga integritet, i takt med att den tekniska utvecklingen på dataområdet fortskridit och uppgifter om medborgarna samlas och bearbetas med hjälp av automatisk databehandling i allt fler sammanhang och allt större uträckning. Mot bakgrund av risken för otillbörliga intrång i den personliga integriteten ansågs det vara väsentligt att visa vilken vikt samhället tillmäter integritetsfrågorna.

Efter en kort genomgång av olika försök i lagstiftning och doktrin att definiera begreppet personlig integritet konstaterade kommittén att det i dessa nästan alltid framhålls ett moment av självbestämmande för den enskilde, inbegripet en rätt för den enskilde att själv bestämma vilka uppgifter om sig själv och sina personliga förhållanden som han ska lämna ifrån sig och även hur dessa uppgifter ska användas och spridas. En annan gemensam utgångspunkt som konstaterades var den enskildes rätt till en fredad sektor.[28]

I betänkandet lyftes fram omständigheter som ansågs vara av betydelse för att få en uppfattning om begreppet integritet. Mot dessa faktorer skulle ställas de krav som samhället har och en rimlig avvägning göras från fall till fall. Enligt kommittén var de omständigheter som främst gjorde sig gällande för den personliga integriteten arten av de personuppgifter som inhämtas och registreras, hur dessa uppgifter används, av vem de används, varför de används, hur de sprids samt mängden av uppgifter som samlas på ett och samma ställe. Vidare framhöll kommittén betydelsen av att de insamlade uppgifterna var korrekta och aktuella.[29]

[27] Data och offentlighetskommitténs delbetänkande *Integritetsskyddet i informationssamhället 3, Grundlagsfrågor* Ds Ju 1987:8.
[28] Ds Ju 1987:8. s. 25.
[29] Ds Ju 1987:8, s. 32.

5.3.4 Skyddet för enskilda personers privatliv – En studie

Justitierådet Per Jermsten fick 1992 i uppdrag att utreda vissa frågor angående skyddet för enskilda personers privatliv. Uppdraget redovisades i departementspromemorian *Skyddet för enskilda personers privatliv – En studie*[30] och inriktades på den personliga integriteten i ideell mening. En särskild anledning till den ökande oron gällande den personliga integriteten som lyftes fram i promemorian var den insamling, lagring och användning av uppgifter om enskilda personer och deras förhållanden som pågick inom både offentlig och privat verksamhet, liksom den ökande ansamlingen av personrelaterade data i register och arkiv. Sett mot bakgrund särskilt av den snabba tekniska utvecklingen i fråga om bl.a. bearbetning och överföring av uppgifter var det enligt utredaren knappast förvånande att oron för ett otillbörligt och kränkande utnyttjande av uppgifterna ökade.

När det sedan gäller den återkommande frågan om vad som avses med begreppet personlig integritet anfördes följande.[31]

> Ifrågavarande problem, som ingalunda är specifikt hos oss, har till en början sin grund i den mångfald förfaranden som kan utgöra eller upplevas som ett angrepp på någons person eller privata sfär. När det sedan gäller att avgränsa vad som ytterst bör ingå i det skyddsvärda området tillkommer den komplikationen att det inte sällan blir fråga om avvägningar som i viss mån beror på upplevelser, känslor och värderingar, dvs. som kan vara påfallande subjektiva. Till detta kommer att uppfattningen om vad som hör, eller bör höra till den personliga integriteten, privatlivets helgd, den privata sfären – eller andra liknande, sammanfattande termer för vad det här ungefär är fråga om – förändras med tidens gång och den allmänna samhällsutvecklingen. Det är med andra ord svårt att ge ett sådant begrepp en tydligare avgränsning än att det innefattar vad som normalt framstår som angeläget att värna om för att den enskilde skall vara tillförsäkrad en rimlig, fredad, privat zon.

5.3.5 Integritetsutredningen

I betänkandet *Personlig integritet i arbetslivet* anförde Integritetsutredningen följande angående vad som egentligen innefattas i begreppet personlig integritet.[32]

---

[30] Ds 1994:51.

[31] Ds 1994:51 s. 8 f.

[32] Integritetsutredningens betänkande *Personlig integritet i arbetslivet*, SOU 2002:18.

Utredningen har gjort en genomgång av åtskillig svensk och utländsk litteratur i ämnet för att söka finna svaret på denna fråga. Det har emellertid visat sig att begreppet personlig integritet inte är så lättfångat. Stora ansträngningar har gjorts för att definiera det men någon kortfattad generell konkretisering av begreppets språkliga innebörd har utredningen inte kunnat finna. Men som en klar gemensam nämnare framstår i vart fall uppfattningen att begreppet personlig integritet innebär att alla människor har rätt till en personlig sfär där ett oönskat intrång, såväl fysiskt som psykiskt, kan avvisas.

De flesta människor har också en bestämd uppfattning om vad personlig integritet innebär för deras egen del och de uttrycker detta mestadels på motsvarande sätt som nyss nämnts. Men uppfattningen om storleken av den privata sfären kan variera kraftigt mellan olika människor beroende framför allt på deras kulturella, etniska, religiösa och sociala bakgrund. Omfånget av den personliga sfären uppfattas inte heller som statiskt, inte ens för den egna individen, utan kan förändras med hänsyn till bl.a. vunna erfarenheter och den aktuella situationen.

5.3.6 Personuppgiftslagsutredningen

I betänkandet Översyn av personuppgiftslagen[33] behandlade Personuppgiftslagsutredningen begreppet personlig integritet, med en särskild inriktning på automatiserad behandling av personuppgifter. Utredningen pekade bl.a. på resultat från undersökningar som visat att människor upplevde det som obehagligt att deras personuppgifter flödade fritt utom deras kontroll, oavsett om uppgifterna i någon mening missbrukades eller om de själva råkade ut för något negativt på grund av att uppgifterna användes.[34] Det framhölls att personlig integritet kan vara att slippa få vissa personliga uppgifter – sådana som det finns rimliga skäl att beteckna som integritetskänsliga – om sig själv spridda till andra människor. Som så många andra konstaterade dock utredningen att svårigheten att definiera begreppet positivt ofta lett till att man i stället försöker identifiera vad som konstituerar en kränkning av den personliga integriteten. Vidare konstaterades att rätten till personlig integritet inte är absolut, utan att skyddet måste vägas mot andra grundläggande rättigheter och värden och under vissa förutsättningar bli föremål för inskränkningar.[35]

[33] Personuppgiftslagsutredningens betänkande Översyn av personuppgiftslagen, SOU 2004:6.
[34] Se även Datalagskommitténs betänkande *Integritet, offentlighet, informationsteknik*, SOU 1997:39 s. 183 f.
[35] SOU 2004:6, s 28 f.

5.3.7 Integritetsskyddskommittén

Integritetsskyddskommittén hade i uppdrag att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten, att överväga om regeringsformens bestämmelse om skydd för den personliga integriteten i 2 kap. 3 § andra stycket borde ändras samt att överväga om det vid sidan av befintlig lagstiftning borde finnas generellt tillämpliga bestämmelser till skydd för den personliga integriteten. Efter en redogörelse över hur begreppet behandlats i tidigare sammanhang, framför allt i olika lagstiftningsarbeten, konstaterade kommittén i sitt slutbetänkande[36] att det inte är möjligt eller i vart fall inte meningsfullt att försöka ge en positiv bestämning av den personliga integriteten, dvs. att formulera en beskrivning som pekar ut alla de situationer i vilka individen har en rätt att få sin integritet respekterad och skyddad. Enligt kommitténs mening kunde det däremot urskiljas vissa moment i den personliga integriteten som är av grundläggande betydelse när rättighetsinskränkande åtgärder övervägs.

> Det måste för det första alltid finnas en rätt till skydd som tar sikte på individens kroppsliga integritet, på den enskildes privata tankar och förtroliga kommunikation med andra samt på den enskildes möjligheter att själv avgöra om andra skall få ta del av känsliga uppgifter som rör t.ex. hälsa eller sexualliv. För det andra måste det alltid finnas ett skydd för rätten att stänga om sig, dvs. utgångspunkten måste vara att den enskilde skall vara fri att kunna avskärma sig från omgivningen. Dessa särskilt viktiga beståndsdelar i skyddet för en människa integritet har utgjort kommitténs principiella utgångspunkter för dess överväganden rörande behovet av ny lagstiftning och vad denna bör ta sikte på.[37]

Efter att ha analyserat lagstiftning som berör den personliga integriteten föreslog Integritetsskyddskommittén bl.a. ett stärkt grundlagsskydd för den personliga integriteten, på så sätt att rätten till personlig integritet gavs självständig betydelse och inte bara – som tidigare – var en funktion av skyddet för främst den fria åsiktsbildningen. Förslaget ledde sedan till att det i 2 kap. 6 § andra stycket regeringsformen infördes en bestämmelse som anger att var och en, utöver vad som i övrigt gäller enligt paragrafen, gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten som görs utan samtycke och innebär övervakning eller kart-

[36] Integritetsskyddskommitténs slutbetänkande *Skyddet för den personliga integriteten, Bedömningar och förslag*, SOU 2008:3.
[37] SOU 2008:3, s. 14 f.

läggning av den enskildes personliga förhållanden. I propositionen anslöt sig regeringen till kommitténs utgångspunkter och anförde bl.a. följande.

> Någon entydig och allmänt accepterad definition av begreppet synes svår att finna. Möjligen kan det sägas att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där intrång bör kunna avvisas. Som Integritetsskyddskommittén framhåller är det emellertid knappast nödvändigt att formulera en allmängiltig definition av begreppet personlig integritet för att kunna bedöma vilka intressen som har ett sådant skyddsvärde att de bör omfattas av ett särskilt starkt skydd mot omotiverade ingrepp. Integritetsskyddskommittén bedömer behovet av ett utökat skydd för den personliga integriteten i första hand utifrån den enskildes intresse av att skydda information om sina personliga förhållanden. Regeringen anser att detta är en rimlig utgångspunkt för en utvidgning av integritetsskyddet i regeringsformen.[38]

Regeringen anförde även att uttrycket information om enskildas personliga förhållanden var avsett att ha samma innebörd som i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400). Som exempel på sådant som kunde omfattas av regleringen nämndes personliga identifikationsuppgifter samt uppgifter om adress, familjeförhållanden, hälsa och vandel, anställning och ekonomi samt fotografiska bilder.[39]

5.4 Personlig integritet i detta betänkande

5.4.1 Begreppets innebörd

Det framstår som mycket tveksamt om någon precis men ändå allmängiltig definition av begreppet personlig integritet är möjlig att slå fast. Än svårare är det att åstadkomma detta i lagstiftning. Skälet till att begreppet inte låter sig fångas i en tydlig sentens är att rätten till en privat sfär inte är absolut, utan relaterad till en rad olika omständigheter, som dessutom kan variera över tid. Kommittén delar därför slutsatsen i tidigare omnämnda Ds 1994:51:

> Det är svårt att ge ett sådant begrepp en tydligare avgränsning än att det innefattar vad som normalt framstår som angeläget att värna om för att den enskilde skall vara tillförsäkrad en rimlig, fredad, privat zon.

[38] Regeringens proposition *En reformerad grundlag*, prop. 2009/10:80 s. 175.
[39] Prop. 2009/10:80 s. 177.

Det kan också konstateras att de flesta länders rättsordningar saknar en sådan definition, även om försök har gjorts på vissa håll.[40] Det kan även ifrågasättas om det finns behov av en exakt definition eller om det mest ändamålsenliga är att från fall till fall avgöra omfattningen av det skydd för integriteten som numera finns uttryckt i regeringsformen.[41] Samtidigt måste innebörden vara tillräckligt tydlig för att det ska vara möjligt att avgöra vad som innebär en kränkning eller ett otillbörligt intrång.

Kommitténs uppdrag att utifrån ett individperspektiv kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten är enligt direktiven begränsat till att omfatta sådana intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik, dvs. i samband med användning av de tekniska möjligheter som skapats genom framsteg inom datorteknik och telekommunikation. Kommitténs kartläggning ska således ta sikte på faktiska och potentiella risker för intrång i *den personliga integriteten i ideell mening*, dvs. i första hand digital insamling, användning och spridning av uppgifter – inklusive bilder – om enskilda och deras personliga förhållanden.

En utgångspunkt för kartläggningen har varit den enskildes rätt till privata tankar och förtrolig kommunikation med andra, samt den enskildes möjligheter att själv avgöra vem som i olika sammanhang ska få ta del av uppgifter som rör denne. I den rätten ligger även ett skydd mot registrering, spridning eller annan behandling av felaktiga, kränkande eller påhittade uppgifter.

5.4.2 Intrång i den personliga integriteten

Modern teknik gör det möjligt att behandla omfattande mängder uppgifter, som förhållandevis enkelt och snabbt också kan få en närapå obegränsad spridning över t.ex. internet. Behandling av personuppgifter med informationsteknik innebär därför särskilt stora risker ur ett integritetsperspektiv.

Intrång i den personliga integriteten kan ha olika syften, göras på olika sätt och av olika aktörer. Ett intrång kan vara såväl legitimt som otillbörligt och det kan också vara förenligt eller oförenligt med

[40] Jfr bl.a. Ds Ju 1987:8 s. 27 f. och SOU 2008:3 s. 14.
[41] Jfr SOU 2007:22 Del 1 s. 52.

gällande lagstiftning. Intrång kan förekomma internt inom en organisation eller göras utifrån. Det kan också göras med uppsåt eller oavsiktligt.

Statens intrång i den personliga integriteten kan, med de utgångspunkter som nämns ovan, bestå i exempelvis en alltför omfattande insamling av uppgifter eller att insamlade uppgifter används för ett ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in. Det kan också handla om att uppgifter behandlas för länge på grund av att gallring inte görs i tid. Staten skulle även kunna begå sådana intrång genom t.ex. hemlig avlyssning, filmning/kameraövervakning och fotografering, övervakning av elektronisk kommunikation samt registrering, spridning och annan behandling av känsliga personuppgifter om t.ex. hälsa och sexualliv.

Privata aktörer, bl.a. enskilda personer och företag, kan begå intrång i den personliga integriteten på motsvarande sätt. En tjänsteleverantör som överför eller lagrar elektronisk kommunikation (t.ex. e-post eller inlägg på sociala medier) kan t.ex. begå intrång genom att samla in, använda eller sprida kundernas kommunikation. Vidare kan enskilda personer kränka andra enskildas personliga integritet genom att exempelvis sprida nedsättande uppgifter om dem, oavsett om uppgifterna i sig är sanna eller påhittade.

Kommitténs bedömning av intrång i den personliga integriteten

När ett intrång i den personliga integriteten ska bedömas måste en avvägning göras utifrån berörda intressen. Faktorer som kommittén avser att beakta vid denna avvägning är bl.a. syftet med och behovet av det aktuella intrånget samt vilken nytta intrånget kan förväntas innebära. Detta ska ställas mot den inverkan som intrånget har för den enskilde. Denna inverkan är bl.a. beroende av graden av känslighet, både avseende uppgifterna som sådana men också intrångets karaktär, jfr t.ex. rumsavlyssning. Sammanhanget och intrångets omfattning är också av betydelse, dvs. hur många drabbas och ifall åtgärden är riktad mot en viss krets eller är helt urskillningslös. Möjligheten att uppnå det önskvärda syftet med hjälp av andra mindre ingripande alternativ bör också bedömas.

Det har betydelse vilken spridning av uppgifter som intrånget innebär. Risken för oönskad spridning har också betydelse för riskbedömningen.

En faktor, som bör vägas in, är risken för att en viss behandling negativt påverkar allmänhetens förtroende i de fall den personuppgiftsansvarige till exempel är en statlig myndighet.

Den enskildes egen inställning till hanteringen av personuppgifter har stor betydelse. När det gäller denna fråga är det förutom frågan om samtycke bl.a. av intresse om den enskilde har rätt till insyn i behandlingen av personuppgifter och möjligheterna till rättelse vid felaktig behandling.

Många intrång i den personliga integriteten är i och för sig befogade. I sådana sammanhang är det av stor vikt att t.ex. lagstiftaren eller en tillämpande myndighet på olika sätt ändå försöker begränsa intrånget. Det kan t.ex. handla om krav på proportionalitet för att en åtgärd ska få vidtas, interna och externa kontrollfunktioner, hur verksamheten organiseras och teknisk säkerhet för information.

I det här delbetänkandet fokuserar vi på risker för den personliga integriteten. I slutbetänkandet återkommer vi med förslag till åtgärder för att hantera riskerna. Då ingår det att väga in flera av de faktorer som nämnts här, som t.ex. nyttan med intrånget.

6 Det grundläggande rättsliga skyddet

6.1 Inledning

Det finns ett stort antal konventioner, EU-direktiv och nationella regleringar som på olika sätt syftar till att skydda den personliga integriteten. I det följande finns en kort beskrivning av de mest grundläggande regleringarna.

6.2 Europakonventionen

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som gäller som lag i Sverige (se även 2 kap. 19 § regeringsformen), innehåller bestämmelser om skydd mot bl.a. kroppsliga ingrepp samt om personlig frihet, rörelsefrihet och egendomsskydd (det sistnämnda i ett tilläggsprotokoll). Enligt artikel 8 gäller vidare att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privatlivet har av Europadomstolen getts en vid tolkning. Skyddet omfattar bl.a. uppgifter om den enskildes identitet, inklusive namn och kön, uppgifter om hälsa och sexuell läggning samt information som rör den personliga utveckningen och relationer till andra individer. Det krävs inte att det är fråga om rent privata relationer, utan skyddet kan även omfatta relationer och aktiviteter som är relaterade till den enskildes yrkesliv.[1] Skyddet gäller även mot angrepp av den enskildes ära och ryktbarhet och mot spridning av information som rör privata förhållanden.[2] Vidare omfattar rätten till

[1] Se t.ex. Rotaru mot Rumänien [GC], nr 28341/95.
[2] Se t.ex. K.U. mot Finland, nr 2872/02, och von Hannover mot Tyskland, nr 59320/00.

respekt för privatlivet ett skydd mot registrering och utlämnande av uppgifter ur allmänna register.[3] Av Europadomstolens praxis framgår vidare att artikel 8 ålägger staten såväl en negativ förpliktelse att avstå från att göra intrång i rätten till respekt för privat- och familjelivet som en positiv förpliktelse att skydda enskilda mot att andra enskilda handlar på ett sätt som innebär integritetsintrång.[4]

Inom Europarådet har även antagits en särskild konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (den s.k. dataskyddskonventionen).

6.3 EU:s rättighetsstadga

Europeiska unionens stadga om de grundläggande rättigheterna, som fogats till Lissabonfördraget, innehåller bestämmelser som är tänkta att återspegla medlemsstaternas gemensamma konstitutionella traditioner och internationella åtaganden när det gäller grundläggande frioch rättigheter. Stadgan innehåller bl.a. bestämmelser om skydd för den personliga integriteten.

I artikel 3 finns ett generellt stadgande om att var och en har rätt till fysisk och mental integritet. Där finns även vissa mer specifika bestämmelser om integritetsskydd inom medicin och biologi, bl.a. ett förbud mot reproduktiv kloning av människor. Enligt artikel 7 har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Vidare innehåller artikel 8 bestämmelser om skydd för personuppgifter. Där anges att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har vidare rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler följs.

[3] Leander mot Sverige, nr 9248/81, och Segerstedt-Wiberg m.fl. mot Sverige, nr 62332/00.

[4] Se t.ex. Airey mot Irland, dom den 9 oktober 1979, Serie A nr 32, samt X och Y mot Nederländerna, dom den 26 mars 1985, Serie A nr 91 och målet E.S mot Sverige, appl. no. 5786/08.

6.4 Regeringsformen

Av målsättningsstadgandet i 1 kap. 2 § regeringsformen framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Vidare innehåller 2 kap. regeringsformen bl.a. bestämmelser om skydd mot kroppsliga ingrepp samt om personlig frihet, rörelsefrihet och egendomsskydd. I 2 kap. 6 § föreskrivs ett skydd mot bl.a. husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Även i övrigt är var och en, enligt samma paragraf, gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten som görs utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. I förarbetena till denna bestämmelse anförs bl.a. att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas.[5]

6.5 Personuppgiftslagen

6.5.1 Dataskyddsdirektivet

Personuppgiftslagen (1998:204) har sin grund i det s.k. dataskyddsdirektivet[6] som antogs 1995. Direktivet genomfördes i Sverige genom personuppgiftslagen och ett antal särregleringar i förhållande till denna lag. Syftet med direktivet är att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter samt att underlätta ett fritt flöde av personuppgifter mellan medlemsstaterna.

På EU-nivå finns även vissa kompletterande rättsakter, bl.a. när det gäller skydd av personuppgifter i frågor som rör polisiärt och straffrättsligt samarbete. Ett exempel på detta är rådets rambeslut

[5] Regeringens proposition *En reformerad grundlag*, prop. 2009/10:80 s. 175; se även Regeringens proposition Översyn av personuppgiftslagen, prop. 2005/06:173 s. 15.

[6] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

2008/977/RIF om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet).

6.5.2 Lagens tillämpningsområde

Genom personuppgiftslagen har dataskyddsdirektivet genomförts i svensk rätt. Personuppgiftslagen gäller vid behandling av personuppgifter i verksamheter som bedrivs av såväl enskilda som av myndigheter. Den gäller däremot inte om en fysisk person behandlar uppgifter helt privat. Lagen innehåller allmänna riktlinjer för behandlingen av personuppgifter, oavsett ändamålet med behandlingen. Personuppgiftslagen ersatte den tidigare datalagen (1973:289).

Personuppgiftslagen är subsidiär i förhållande till annan lagstiftning, vilket innebär att om det i en annan lag eller i en förordning finns bestämmelser som avviker från denna lag, ska de andra bestämmelserna gälla. Sådana avvikande bestämmelser finns på en rad olika områden och är ofta begränsade till ett visst verksamhetsområde, en viss typ av register eller för ett särskilt register. Som exempel på sådana registerförfattningar kan nämnas lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, patientdatalagen (2008:355) och polisdatalagen (2010:361). Utgångspunkten har varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag.[7]

6.5.3 Grundläggande krav för behandlingen

I 9 § personuppgiftslagen anges vissa grundläggande krav för all behandling av personuppgifter. Det är den personuppgiftsansvarige som gentemot den registrerade ansvarar för att dessa grundläggande krav alltid uppfylls vid behandlingen.

Personuppgifter får behandlas bara om det är lagligt och behandlingen ska alltid göras på ett korrekt sätt och i enlighet med god sed. Insamling och annan behandling av personuppgifter får endast göras för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålen med en behandling av personuppgifter måste alltså bestämmas

[7] Se t.ex. Regeringens proposition *Om offentlighet, integritet och ADB*, prop. 1990/91:60 s. 58.

redan när uppgifterna samlas in. Det eller de ändamål som anges får inte vara alltför allmänt hållna. Som exempel kan nämnas att det har ansetts otillräckligt att ange kontroller som ändamål för loggning och övervakning; även syftet med kontrollerna måste anges med t.ex. övervakning av tekniska och säkerhetsmässiga skäl eller uppföljning av att interna regler följs.[8]

Enligt den s.k. finalitetsprincipen får uppgifterna efter att de samlats in inte behandlas för något ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in. Det innebär t.ex. att uppgifter om anställda som samlas in för att utgöra underlag för prestationslön inte får användas för att i realtid övervaka hur de utför sina arbetsuppgifter och när de tar raster.[9] Det innebär också att möjligheterna till s.k. samkörning av register begränsas. Vidare följer en skyldighet för den personuppgiftsansvarige att under hela tiden som uppgifterna behandlas hålla reda på för vilka ändamål varje personuppgift har samlats in.[10] Den personuppgiftsansvarige anses vara skyldig att se till att personuppgifter för olika ändamål inte blandas.[11]

Det krävs inte att en registrerad samtycker till eventuell behandling för nya ändamål som inte är oförenliga med det ursprungliga ändamålet eller att ny information lämnas till den registrerade. Ett utlämnande av personuppgifterna till annan måste emellertid vara förenligt med de ursprungliga ändamålen. Vid bedömningen av detta krävs att man beaktar vad den som vill ha ut uppgifterna ska använda dem till och jämföra den tilltänkta användningen med de ursprungliga ändamålen.[12] Den som har fått ut uppgifterna anses däremot inte vara bunden av de ändamål som ursprungligen bestämts av den personuppgiftsansvarige som lämnat ut uppgifterna.[13]

Det finns vidare krav på att personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Det innebär att ovidkommande uppgifter inte får behandlas. De behandlade personuppgifterna ska vidare vara riktiga och aktu-

[8] Datainspektionens rapport 2005:3 s. 14.
[9] Datainspektionens beslut den 27 juni 2007, dnr 87-2207.
[10] Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen – En kommentar, fjärde upplagan, s. 203.
[11] Regeringens proposition *Omreglering av apoteksmarknaden*, prop. 2008/09:145 s. 336.
[12] Regeringens proposition *Effektivare pantbrevshantering m.m*, prop. 2002/03:57 s. 26).
[13] Öman och Lindblom, s. 204.

ella. Uppgifterna får inte heller vara fler än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Även för bedömningen av detta krävs att ändamålet har preciserats i tillräcklig grad.

Om kraven på behandlingen av personuppgifter inte uppfylls ska den personuppgiftsansvarige vidta alla rimliga åtgärder för att utplåna, blockera eller rätta uppgifterna.

Slutligen gäller att personuppgifter inte får sparas längre än nödvändigt med hänsyn till de ändamål för vilka de behandlas. Därefter ska uppgifterna avidentifieras eller förstöras. Behandling för historiska, statistiska eller vetenskapliga ändamål får dock pågå under längre tid än vad som är nödvändigt med hänsyn till de ursprungliga ändamålen.

6.5.4 Tillåten behandling

Personuppgiftslagen innehåller en uttömmande uppräkning av under vilka förutsättningar behandling av personuppgifter är tillåten (10–12 §§). Som utgångspunkt gäller att personuppgifter endast får behandlas om den registrerade har lämnat sitt samtycke till det. Samtycket måste lämnas innan behandlingen påbörjas.[14] Har den registrerade inte lämnat sitt samtycke till behandlingen krävs att den är nödvändig för något av vissa i lagen angivna ändamål. Det kan vara för att fullgöra ett avtal med den registrerade eller för att fullgöra en rättslig skyldighet, men också när det krävs för att vitala intressen för den registrerade ska kunna skyddas eller för att en arbetsuppgift av allmänt intresse ska kunna utföras. Slutligen får personuppgifter även behandlas om en intresseavvägning ger vid handen att den personuppgiftsansvariges berättigade intresse av en behandling väger tyngre än den registrerades intresse av integritetsskydd. Som exempel på tillämpning av nämnda bestämmelse kan nämnas att Datainspektionen efter en intresseavvägning har ansett att det av trafiksäkerhetsskäl är tillåtet att logga personuppgifter om utandningsprov som lämnats av bl.a. bussförare i samband med arbetspass.[15]

Av 13 § personuppgiftslagen följer ett förbud mot behandling av känsliga personuppgifter. Känsliga personuppgifter definieras som uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter,

[14] Jfr NJA 2005 s. 361.
[15] Datainspektionens beslut den 12 januari 2011, dnr 500-2010.

religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Förbudet omfattar enligt 5 a § inte personuppgifter som inte ingår i eller är avsedda att ingå i strukturerat material, dvs. en samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier.

I 14–19 §§ anges ett antal fall då känsliga uppgifter får behandlas trots förbudet i 13 §. Känsliga personuppgifter får till att börja med behandlas om den registrerade har samtyckt till behandlingen eller på ett tydligt sätt offentliggjort uppgifterna. Vidare får känsliga personuppgifter behandlas om det är nödvändigt med hänsyn till vissa särskilt angivna ändamål, t.ex. för att den registrerades eller någon annans vitala intressen ska kunna skyddas och den registrerade inte kan lämna samtycke till behandlingen, eller för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras. Det finns även undantag för ideella organisationer med vissa syften. Omfattande undantag gäller också i fråga om behandling av känsliga personuppgifter för hälso- och sjukvårdsändamål samt för forsknings- och statistikändamål. Dessutom finns utrymme för regeringen, eller den myndighet regeringen bestämmer, att enligt 20 § meddela föreskrifter om ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse. Sådana föreskrifter finns i 8 § personuppgiftsförordningen (1998:1191). Enligt den bestämmelsen får myndigheter generellt behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ärendet.

Enligt 21 § personuppgiftslagen är det som huvudregel förbjudet för andra än myndigheter att behandla sådana personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Uppgifter om personnummer och samordningsnummer får enligt 22 § behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Med hänsyn till vikten av säker identifiering har det t.ex. ansetts motiverat att behandla personnummer i bl.a. vårdregister, inom socialtjänsten och i kreditupplysningsverksamhet.[16]

[16] Öman och Lindblom s. 347 med hänvisningar.

6.5.5 Information och rättelse

I 23–27 §§ personuppgiftslagen finns bestämmelser som syftar till att trygga den enskildes rätt att kontrollera om behandling av personuppgifter om honom eller henne pågår. Om uppgifterna samlas in från personen själv ska den personuppgiftsansvarige självmant lämna information till den registrerade om behandlingen av uppgifterna. Har uppgifterna samlats in från någon annan än den enskilde, ska han eller hon informeras när uppgifterna registreras, eller, om avsikten med behandlingen är att lämna ut dem till tredje man, när uppgifterna lämnas ut första gången. Information behöver dock inte lämnas om det finns bestämmelser om registrerandet eller utlämnande av uppgifterna i författning eller om det skulle vara omöjligt eller kräva en oproportionerligt stor arbetsinsats att informera. Informationen ska omfatta uppgift om vem som är personuppgiftsansvarig, ändamålet med behandlingen samt all övrig information som den registrerade behöver för att kunna ta tillvara sina rättigheter i samband med behandlingen. Den personuppgiftsansvarige är vidare skyldig att efter ansökan, en gång per år, gratis informera om ifall, och i så fall vilka uppgifter om sökanden som behandlas, ändamålet med behandlingen, varifrån uppgifterna kommer och till vem de lämnas ut. Uppgiftsskyldigheten omfattar dock inte alla uppgifter, bl.a. inte uppgifter som omfattas av sekretess eller tystnadsplikt gentemot den registrerade.

Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen, ska enligt 28 § på begäran av den registrerade rättas, utplånas eller blockeras av den personuppgiftsansvarige. Om felaktiga personuppgifter har lämnats ut till tredje man, ska denne i vissa fall informeras om korrigeringen.

6.5.6 Säkerhet vid behandlingen

I 31 § personuppgiftslagen finns bestämmelser om säkerhet vid behandling av personuppgifter. Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjlig-

heter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur känsliga de behandlade personuppgifterna är.

De tekniska möjligheterna handlar om vilka hjälpmedel som finns tillgängliga på marknaden. Tekniska system kan bl.a. innehålla funktioner för behörighetskontroll, förande av behandlingshistorik såsom loggning, och kryptering. De särskilda risker som finns med en behandling kan exempelvis vara beroende av antalet personer som de behandlade uppgifterna rör.[17] Känsligheten hos personuppgifterna kan handla om arten hos de personuppgifter som behandlas, men även om andra faktorer som t.ex. mängden av uppgifter om enskilda personer.

Datainspektionen har utfärdat allmänna råd om säkerhet för personuppgifter. I dessa råd anges bl.a. att en personuppgiftsansvarig bör ha en fastställd säkerhetspolicy, i vart fall om en omfattande behandling av personuppgifter utförs eller om känsliga personuppgifter behandlas, samt att kontroller bör genomföras för att säkerställa att riktlinjer och regler följs. Det kan bl.a. handla om system för behörighetskontroll, för att säkerställa vilka anställda som får del av åtkomstskyddade personuppgifter. Det bör vidare finnas rutiner för rapportering och uppföljning av säkerhetsincidenter.[18]

Det är den personuppgiftsansvarige som ansvarar för säkerheten. Om ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige förvissa sig om att biträdet kan genomföra de säkerhetsåtgärder som måste vidtas och att se till att det verkligen görs. Även om den faktiska behandlingen av uppgifterna överlåts, så kvarstår alltid det yttersta ansvaret hos den personuppgiftsansvarige.

6.5.7 Överföring av personuppgifter till tredje land

Enligt 33 § personuppgiftslagen är det förbjudet att föra över personuppgifter till tredje land om landet inte har en adekvat nivå för skyddet av personuppgifter. Förbudet gäller också överföring av personuppgifter för behandling i tredje land. Bestämmelsen gäller däremot inte vid behandling av personuppgifter i ostrukturerat material. Den som uppsåtligen eller av grov oaktsamhet kränker den registrerades

[17] Öman och Lindblom s. 437 f.
[18] Se vidare Datainspektionens allmänna råd – Säkerhet för personuppgifter.

personliga integritet genom att föra över personuppgifter till tredje land som inte har en adekvat skyddsnivå kan göra sig skyldig till brott mot personuppgiftslagen (se nedan).

Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen i det enskilda fallet. I paragrafen anges att särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet.

I 34 § anges ett antal undantag från förbudet i 33 §. Det är bl.a. tillåtet att föra över personuppgifter till tredje land om den registrerade har lämnat sitt samtycke därtill eller om överföringen är nödvändig för vissa närmare angivna syften, bl.a. för att den registrerades vitala intressen ska kunna skyddas. Vidare är det tillåtet att föra över personuppgifter för användning i en stat som har anslutit sig till Europarådets dataskyddskonvention. I 35 § finns bemyndiganden som framför allt ger regeringen möjlighet att besluta om ytterligare undantag från förbudet i 33 §.

6.5.8 Kommande lagstiftning

Den 15 december 2015 kom EU-kommissionen, Europaparlamentet och EU:s ministerråd överens om ett förslag till ny EU-förordning om dataskydd som ska ersätta såväl dataskyddsdirektivet som personuppgiftslagen. Europaparlamentet beslutade den 16 april 2016 att anta förordningen. Förordningen publicerades den 4 maj 2016 i Europeiska unionens officiella tidning med den korta benämningen ”allmän dataskyddsförordning”.[19] Förordningen ska tillämpas från och med den 25 maj 2018. Syftet med förordningen har framför allt varit att ytterligare harmonisera och effektivisera skyddet av personuppgifter för att förbättre den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. Förordningen är direkt tillämplig i medlemsstaterna.

[19] Den fullständiga benämningen är Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Den 4 maj 2016 publicerades även det direktiv som ska ersätta dataskyddsrambeslutet (rambeslut 2008/977/RIF).[20] Direktivet omfattar, till skillnad från dataskyddsrambeslutet, inte endast utbyte av information över gränserna, utan även nationell personuppgiftsbehandling inom den brottsbekämpande sektorn. Medlemsstaterna ska, som huvudregel, senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa direktivet samt börja tillämpa dessa bestämmelser från och med den 6 maj 2018.

6.6 Lagen om elektronisk kommunikation

I lagen (2003:389) om elektronisk kommunikation finns bl.a. bestämmelser om integritetsskydd vid tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster samt vid abonnentupplysning. Regleringen bygger på Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation).

Av 6 kap. 5, 6 och 8 §§ lagen om elektronisk kommunikation framgår att bl.a. tele- och internetleverantörer enligt huvudregeln ska utplåna eller avidentifiera trafikuppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande. Det finns dock flera undantag från denna princip. Uppgifterna får bl.a. sparas när det är nödvändigt för att kunna förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. De får även sparas om de behövs för abonnentfakturering eller för betalning av avgifter för samtrafik. Om en abonnent eller användare har samtyckt till det, får uppgifterna också behandlas för att marknadsföra elektroniska kommunikationstjänster. Lagen om elektronisk kommunikation innehåller även bestämmelser om bl.a. säkerhet och tystnadsplikt samt ett förbud mot avlyssning. Av regleringen framgår bl.a. att många lagrade uppgifter endast får lämnas ut när domstol har beslutat om det.

[20] Det nya direktivets fullständiga benämning är Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

I direktivet om integritet och elektronisk kommunikation finns även bestämmelser som innebär att medlemsstaterna under vissa närmare angivna förutsättningar får införa andra undantag från skyldigheten att utplåna eller avidentifiera trafikuppgifterna när de inte längre behövs för att överföra ett elektroniskt meddelande. Det var med stöd av den regleringen som bl.a. Sverige införde en skyldighet för bl.a. tele- och internetleverantörer att under viss tid lagra trafikuppgifter för brottsbekämpande ändamål (se 6 kap. 16 a § lagen om elektronisk kommunikation samt t.ex. Ds 2014:23).

Europaparlamentets och rådets direktiv (2006/24/EG) om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät (Datalagringsdirektivet) införlivades den 1 maj 2012 i svensk rätt. Datalagringsdirektivet syftar till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra trafik- och lokaliseringsuppgifter samt uppgifter som behövs för att identifiera en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott.

Den 8 april 2014 ogiltigförklarade EU-domstolen[21] Datalagringsdirektivet i sin helhet. Domstolens ogiltigförklaring gäller med retroaktiv verkan från den dag direktivet trädde i kraft. Domstolen anser att Datalagringsdirektivet utgör ett synnerligen allvarligt ingrepp i den grundläggande rätten till respekt för privatlivet och skydd för personuppgifter genom att kräva att dessa uppgifter ska lagras och genom att ge behöriga nationella myndigheter tillgång till dessa uppgifter. Lagringen av uppgifter i syfte att eventuellt överlämna dem till behöriga nationella myndigheter svarar mot ett mål av allmänt intresse nämligen bekämpningen av grov brottslighet som syftar till allmän säkerhet. Domstolen anser dock att unionslagstiftaren genom att anta Datalagringsdirektivet har överskridit de gränser som följer av proportionalitetsprincipen.

Datalagringsutredningen[22] har därefter gjort bedömningen att det svenska regelverket om lagring och utlämnande av uppgifter ryms inom de ramar som ställs upp av unions- och europarättens allmänna principer och kravet på respekt för grundläggande rättigheter. I be-

[21] Dom den 8 april 2014 i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl.
[22] *Datalagring, EU-rätten och svensk rätt* (Ds 2014:23).

tänkandet *Datalagring och integritet*[23] har dock utredningen föreslagit vissa lagändringar i syfte att stärka skyddet för den personliga integriteten när det gäller lagring av uppgifter om elektronisk kommunikation för brottsbekämpande ändamål.

6.7 Tillsyn

6.7.1 Inledning

Datainspektionen har det övergripande ansvaret för att värna skyddet för enskildas personliga integritet vid behandling av personuppgifter. Som framgår av det följande utövas dock viss tillsyn primärt av andra myndigheter.

6.7.2 Datainspektionen

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen och har bl.a. i uppgift att värna skyddet för enskildas personliga integritet vid behandling av personuppgifter. Myndigheten har också ett centralt tillsynsansvar för all kameraövervakning.

Datainspektionen har för sin tillsyn rätt att på begäran få tillgång till de personuppgifter som behandlas samt upplysningar och dokumentation av behandlingen och säkerheten vid denna. Datainspektionen har även rätt att få tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Om Datainspektionen inte efter begäran kan få tillräckligt underlag för att konstatera att behandlingen är laglig får den vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på annat sätt än att lagra dem. Vite används dock i regel inte mot statliga myndigheter.[24]

Om Datainspektionen konstaterar att uppgifter behandlas eller kan komma att behandlas på ett olagligt sätt ska tillsynsmyndigheten, genom påpekanden eller liknande förfaranden, försöka åstadkomma rättelse. Går det inte att få rättelse på annat sätt, eller om saken är brådskande, får myndigheten på motsvarande sätt förbjuda

[23] Datalagringsutredningens betänkande *Datalagring och integritet*, SOU 2015:31.

[24] Regeringens propositioner *Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling*. prop. 2004/05:164 s. 54 och *Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt*, prop. 2006/07:46 s. 105; jfr Regeringens proposition *Effektivare sanktioner för arbetsmiljö- och arbetstidsreglerna* prop. 2012/13:143 s. 67 f.

annan behandling än lagring. Datainspektionen får också ansöka hos förvaltningsrätten om att sådana uppgifter som har behandlats på olagligt sätt ska utplånas.

6.7.3 Övriga tillsynsmyndigheter

Konsumentverket utövar tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden. *Konsumentombudsmannen* kan utfärda förelägganden och inleda rättsprocesser mot företag som bryter mot den lagen.

Riksdagens ombudsmän (Justitieombudsmannen) är en myndighet under riksdagen och en del av riksdagens kontrollmakt. Justitieombudsmannen har bl.a. i uppgift att se till att myndigheter och domstolar följer regeringsformens bestämmelser om opartiskhet och saklighet samt att den offentliga verksamheten inte gör intrång i medborgarnas grundläggande fri- och rättigheter. I tillsynsarbetet ingår bl.a. att kontrollera att myndigheterna handlägger sina ärenden och i övrigt utför sina uppgifter enligt gällande författningar.

Justitiekanslern (JK) utövar tillsyn över myndigheter och deras tjänstemän. Tillsynen syftar till att kontrollera att lagar och andra författningar följs och är främst inriktad på att upptäcka systematiska fel i den offentliga verksamheten.

Post- och telestyrelsen har i uppdrag att utöva tillsyn över behandling av uppgifter vid elektronisk kommunikation. Länsstyrelserna utöver tillsyn när det gäller kameraövervakning av platser dit allmänheten har tillträde. Det finns även sektorsspecifika myndigheter som utövar tillsyn, t.ex. *Inspektionen för vård och omsorg*, *Säkerhets- och integritetsskyddsnämnden* samt *Statens inspektion för försvarsunderrättelseverksamheten*.

6.7.4 Pågående arbete

Regeringen har tillsatt *Utredningen om en myndighet med ett samlat ansvar för tillsyn över den personliga integriteten*[25], som har i uppdrag att bl.a. överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur. Uppdraget ska redovisas senast den 30 september 2016.

6.8 Sanktioner

6.8.1 Inledning

I svensk rätt finns inte något generellt straffskydd mot integritetskränkningar.[26] Som framgår av det följande finns däremot straffbestämmelser i framför allt brottsbalken och personuppgiftslagen som omfattar vissa överträdelser. Antalet polisanmälningar som rör brott mot personuppgiftslagen är dock förhållandevis få. Se vidare kapitel 24. När det gäller förhållandet mellan enskilda är därför de generella straffbestämmelserna i framför allt brottsbalken av störst praktisk betydelse för skyddet för den personliga integriteten. Som framgår nedan finns därutöver vissa möjligheter för den som utsatts för ett integritetsintrång att få skadestånd.

6.8.2 Brott mot personuppgiftslagen

I 49 § personuppgiftslagen finns en bestämmelse om straff för den som bryter mot vissa bestämmelser i lagen. För *brott mot personuppgiftslagen* döms till att börja med den som behandlar känsliga personuppgifter och uppgifter om lagöverträdelser i strid med bestämmelserna i 13–21 §§. Det är även straffbart att i ostrukturerat material behandla sådana uppgifter om det innebär att den registrerades personliga integritet kränks (jfr 5 a § andra stycket). Vidare kan den som för över personuppgifter till tredje land i strid med bestämmelserna i 33–35 §§ dömas för brott mot personuppgiftslagen. Även

[25] Dir. 2014:164 och dir. 2015:139.

[26] Yttrandefrihetskommittén har däremot i betänkandet *En översyn av tryck- och yttrandefriheten* (SOU 2012:55) gjort bedömningen att det finns ett tydligt behov av en generell straffbestämmelse utanför det grundlagsskyddade området och att det finns skäl för regeringen att överväga en sådan bestämmelse (s. 433 f.).

när det gäller personuppgifter i ostrukturerat material kan en överföring till tredje land utan adekvat skyddsnivå vara straffbar, om den innebär en kränkning av den registrerades personliga integritet. Slutligen döms den för brott mot personuppgiftslagen som lämnar osann uppgift i sådan information till registrerade som föreskrivs i lagen, i anmälan till tillsynsmyndighet eller till tillsynsmyndighet som begär information (43 §). Detsamma gäller den som låter bli att fullgöra skyldigheten enligt framför allt 36 § att anmäla personuppgiftsbehandling till tillsynsmyndighet.

För straffbarhet krävs uppsåt eller grov oaktsamhet. Det är den fysiska personen som har gjort sig skyldig till förfarandet, eller i vissa fall underlåtenheten, som döms för brott, oavsett om han eller hon är personuppgiftsansvarig. Om ett brott har begåtts inom ramen för en näringsverksamhet kan företagsbot enligt 36 kap. 7 § brottsbalken bli aktuellt för näringsidkaren.

Påföljden för brott mot personuppgiftslagen är böter eller fängelse i högst sex månader eller, om brottet är grovt, fängelse i högst två år. I ringa fall döms inte till ansvar.

Straffansvaret gäller inte i medier som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Genom att ansöka om utgivningsbevis hos Myndigheten för radio och tv för en databas som innehåller personuppgifter, kan var och en få grundlagsskydd för databasen och därigenom utesluta en tillämpning av personuppgiftslagen. *Mediegrundlagskommittén*[27] har dock i uppdrag att bl.a. överväga om någon förändring bör göras i detta avseende.

6.8.3 Straffbestämmelser i bl.a. brottsbalken

Behandling av personuppgifter kan i vissa fall utgöra brott enligt annan lagstiftning, t.ex. brottsbalken. Det gäller framför allt brott som innebär ett angrepp på annans frid, anseende eller ära. Vissa bestämmelser straffbelägger anskaffning, användning eller spridning av information om privata förhållanden. Andra bestämmelser straffbelägger själva intrånget i den fredade sektor där enskilda anses ha rätt att avvisa utomståendes inblandning.

[27] Dir. 2014:97.

När det gäller anskaffning av information kan till att börja med nämnas bestämmelsen i 4 kap. 9 c § brottsbalken om *dataintrång*. Där framgår att det är straffbart att olovligen bereda sig tillgång till uppgift som är föremål för automatisk behandling. Det är vidare straffbart att olovligen ändra, utplåna, blockera eller i register föra in en sådan uppgift. Med *uppgift som är avsedd för automatiserad behandling* avses alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för dator anpassad och läsbar form, men också program av olika slag och uppgifter som finns i en dators temporära minne, liksom uppgifter som är under befordran, oavsett på vilket sätt en sådan befordran görs.[28] Bestämmelsen förutsätter inte att intrånget görs i ett visst syfte, t.ex. för att hämta information eller för att åstadkomma skada eller någon annan följd. Vad som beläggs med straff är själva intrånget. För straffansvar förutsätts inte heller att någon säkerhetsåtgärd kringgås.[29] Exempelvis en anställd som av nyfikenhet olovligen läser uppgifter i en databas, kan alltså göra sig skyldig till dataintrång.

Enligt 4 kap. 9 a § brottsbalken döms den som olovligen, med hjälp av ett tekniskt hjälpmedel för återgivning av ljud, i hemlighet avlyssnar eller upptar tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, till vilken allmänheten inte äger tillträde och som han själv inte deltar i eller som han har berett sig tillträde till utan att ha behörighet till detta för *olovlig avlyssning*. Bestämmelsens skyddar alltså dels mot avlyssning eller upptagning av tal i enrum – t.ex. diktamen eller bön – dels samtal mellan andra. Det är inte straffbart att spela in samtal som man själv deltar i, oavsett om de andra deltagarna känner till inspelningen eller inte. Straffet för olovlig avlyssning är böter eller fängelse i högst två år.

Sedan år 2013 är det även straffbart att olovligen och i hemlighet fotografera den som befinner sig i en bostad eller på en toalett, i ett omklädningsrum eller ett liknande utrymme (4 kap. 6 a § brottsbalken). Sådan *kränkande fotografering* anses innebära ett intrång i den fredade sfär som enskilda personer bör ha rätt till i förhållande till andra enskilda. Straffet är böter eller fängelse i högst två år.

[28] Regeringens proposition *Angrepp på informationssystem*, Prop. 2006/07:66 s. 49.
[29] Nils-Olof Berggren m.fl., *Brottsbalken – en kommentar*, kommentar till BrB 4:9 c s. 5.

Gärningen är dock ansvarsfri om den med hänsyn till syftet och övriga omständigheter är försvarlig. Det är inte heller brottsligt att i som led i en myndighets verksamhet ta upp bild av någon.

Den som olovligen bereder sig tillgång till ett meddelande som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller i ett elektroniskt kommunikationsnät döms *för brytande av post- och telehemlighet* till böter eller fängelse i högst två år (4 kap. 8 § brottsbalken).

Den som ”lyfter vapen mot annan eller eljest hotar med brottslig gärning på sätt som är ägnat att hos den hotade framkalla allvarlig fruktan för egen eller annans säkerhet till person eller egendom” döms enligt 4 kap. 5 § brottsbalken för *olaga hot* till böter eller fängelse i högst ett år. Gärningen kan bl.a. begås med hjälp av informationsteknik, exempelvis via e-post. Om brottet är grovt är straffet fängelse lägst sex månader och högst fyra år.

För *ofredande* döms den som ”handgripligen antastar eller medelst skottlossning, stenkastning, oljud eller annat hänsynslöst beteende ofredar annan”, till böter eller fängelse i högst ett år (4 kap. 7 § brottsbalken). En gärning ska anses innebära ett ofredande genom hänsynslöst beteende om den enligt en vanlig värdering kan sägas utgöra en kännbar integritetskränkning.[30]

Det finns inte något generellt förbud för enskilda att lämna eller sprida integritetskänsliga uppgifter. I vissa fall kan dock spridning av nedsättande uppgifter eller integritetskänsliga bilder däremot straffas som förtal. Enligt 5 kap. 1 § brottsbalken döms den för *förtal* som pekar ut en annan person som brottslig eller klandervärd i sitt levnadssätt eller som på något annat sätt lämnar en uppgift som är ägnad att utsätta denne för andras missaktning. Brottet består alltså i att en person till en annan person lämnar en nedsättande uppgift om en tredje person. En uppgift kan lämnas genom tal och skrift men även genom t.ex. en bild.[31] Från straffansvaret undantas fall när den som lämnat uppgiften varit skyldig att uttala sig eller om det annars med hänsyn till omständigheterna varit försvarligt att lämna uppgiften. I båda fallen måste den som lämnat uppgiften visa att upp-

[30] NJA II 1962 s. 134.

[31] I NJA 1992 s. 594 hade den tilltalade utan målsägandens vetskap videofilmat ett samlag mellan dem och därefter visat filmen för flera personer. Visandet av filmen bedömdes som grovt förtal.

giften varit sann eller att uppgiftslämnaren hade skälig grund för den. Straffet för förtal är böter. För grovt förtal döms till böter eller fängelse i högst två år.

För *förolämpning* döms den som ”smädar annan genom kränkande tillmäle eller beskyllning eller genom annat skymfligt beteende mot honom” till böter, eller om brottet är grovt till böter eller fängelse i högst sex månader. Bestämmelsen tar sikte på kränkningar av någons ära som riktar sig direkt till den som berörs.

Även andra brott kan begås med användning av informationsteknik, exempelvis *sexuellt ofredande*, *olaga förföljelse*, övergrepp i rättssak, *brott mot tystnadsplikt*, överträdelse av kontaktförbud, *barnpornografibrott* och *olaga våldskildring*.

Därutöver har den som tillhandahåller en tjänst för elektronisk förmedling av meddelanden ett ansvar för att ta bort meddelanden från tjänsten, eller på annat sätt förhindra vidare spridning av meddelanden som bl.a. uppenbart utgör hets mot folkgrupp eller barnpornografibrott (5 § lagen [1998:112] om *ansvar för elektroniska anslagstavlor*). Den som uppsåtligen eller av grov oaktsamhet bryter mot nämnda skyldighet döms enligt 7 § till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år. I ringa fall döms dock inte till ansvar.

När det gäller medier som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen gäller dock vissa begränsningar av straffansvaret, se 7 och 8 kap. tryckfrihetsförordningen respektive 5 och 6 kap. yttrandefrihetsgrundlagen.

Slutligen bör nämnas att *Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten*[32] har haft i uppdrag att se över det straffrättsliga skyddet för enskildas personliga integritet, särskilt när det gäller hot och andra kränkningar. Utöver befintliga regler om olaga hot, ofredande, förtal och förolämpning har utredningen ta ställning till om det straffrättsliga skyddet bör kompletteras när det gäller spridning av integritetskränkande uppgifter utanför det grundlagsskyddade området (dvs. sådant som inte regleras i tryckfrihetsförordningen och yttrandefrihetsgrundlagen). Utredningen har vidare övervägt om det bör införas ett straffansvar för den som tillhandahåller en elektronisk anslagstavla och som inte tar bort

[32] Ju 2014:10, dir. 2014:74.

eller på annat sätt förhindrar spridning av meddelanden som kränker enskildas personliga integritet. Utredningens förslag presenterades i februari 2016.[33] Mer om utredningens förslag redovisas i avsnitt 23.1.

6.8.4 Skadestånd

Om behandling av personuppgifter i strid med personuppgiftslagen orsakar skada eller kränkning av den personliga integriteten för den registrerade har han eller hon, enligt 48 § personuppgiftslagen, rätt till skadestånd från den personuppgiftsansvarige. Skadeståndsansvaret åligger som huvudregel just den personuppgiftsansvariga och inte t.ex. den anställda som vidtagit en viss åtgärd, eventuella personuppgiftsbiträden eller personuppgiftsombud. Skadeståndsansvaret är i princip strikt, vilket innebär att det inte krävs att den personuppgiftsansvarige eller någon annan har haft uppsåt att handla i strid med lagen eller varit oaktsam. Den registrerade behöver bara visa att det förekommit en felaktig behandling och att denna skadat eller kränkt honom eller henne. Omständigheter som kan ha betydelse vid bedömningen av om det har förekommit en kränkning är bl.a. vilka personuppgifter som behandlas, graden av känslighet hos uppgifterna, i vilket sammanhang uppgifterna förekommer, för vilket syfte uppgifterna behandlas, vilken spridning uppgifterna har fått eller riskerat att få samt vad behandlingen kan leda till.

Ersättningen kan i den utsträckning det är skäligt sättas ned, helt eller delvis, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. Det kan t.ex. handla om att det är den registrerade som har t.ex. lämnat felaktiga eller ofullständiga personuppgifter vilket lett till den olagliga behandlingen.

Det finns även möjlighet att erhålla skadestånd för kränkning vid brottslig gärning, enligt den allmänna regleringen i 2 kap. 3 § *skadeståndslagen* (1972:207). För att sådant skadeståndsansvar ska komma i fråga krävs att kränkning varit allvarlig. Vidare gäller ansvaret endast vid vissa typer av brott, nämligen angrepp på annans person, mot annans frihet samt mot annans frid eller ära. De två sistnämnda kategorierna är av störst intresse här. Brott mot annans frid avser den enskildes rätt att vara i fred och hålla sitt privatliv okänt för andra.

[33] Utredningens om ett modernt och starkt straffrättsligt skydd för den personliga integriteten betänkande *Integritet och straffskydd*, SOU 2016:7.

Som exempel kan nämnas olaga hot, ofredande, brytande av post- och telehemlighet samt olovlig avlyssning. Angrepp mot annans ära avser i första hand ärekränkningsbrott, t.ex. förtal.

Om den personliga integriteten har kränkts på ett sätt som strider mot Regeringsformen eller Europakonventionen kan det även finnas en rätt till skadestånd som grundas direkt på dessa regelverk.[34]

När det gäller medier som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen gäller dock vissa begränsningar i skadeståndsansvaret, se 11 kap. tryckfrihetsförordningen respektive 8 kap. yttrandefrihetsgrundlagen.

[34] NJA 2005 s. 462 och NJA 2014 s. 323.

DEL III

Riskbedömning av olika områden och företeelser

7 Skolan

Kommitténs bedömning: De olika företeelser som vi har kartlagt inom skolans område är förknippade med risker av olika allvarlighetsgrad; såväl vissa risker, påtagliga risker och allvarliga risker kan konstateras. Läs mer om hur vi bedömt riskerna avseende de olika företeelserna i avsnitt 7.7.

7.1 Inledning

7.1.1 Beskrivning av området

Det här kapitlet är inriktat på skolan. Det berör endast i mycket liten utsträckning förhållandena vid universitet och högskolor.

Skolan är snabbt på väg att digitaliseras, i den meningen att allt fler IKT-verktyg[1] börjar användas av allt fler elever och lärare. Det rör sig om en uppsjö av sinsemellan helt olika verktyg som digitala lärplattformar, digitala läromedel, sociala medier osv.

Verktygen används för praktiska och pedagogiska ändamål och syftar till att förbättra undervisningen och underlätta lärandet, både för den enskilde eleven och för elevkollektivet. Men en ökad användning av digitala verktyg innebär också att fler uppgifter om eleverna hanteras av skolorna och tjänsteleverantörerna.

Digitaliseringen av skolan kan mätas på olika sätt – ett vanligt förekommande mått är antalet datorer i skolan och hur dessa används i undervisningen.

[1] IKT står för informations- och kommunikationsteknik.

Skolverkets senaste uppföljning av it-användning och it-kompetens visar att det under de senaste åren skett en stor ökning av antalet datorer i såväl förskola, grundskola som gymnasieskola.[2]

Antalet skolor som använder sig av internetbaserade lärplattformar för samarbetet mellan elever och lärare har också ökat. År 2015 användes sådana av 67 procent av de kommunala grundskolorna (56 procent av de fristående grundskolorna) och av 95 procent av de kommunala gymnasieskolorna (84 procent av de fristående gymnasieskolorna).

Många skolor, sju av tio grundskolor och åtta av tio gymnasieskolor, använder i dag s.k. molntjänster som t.ex. Google apps, Office 365 och iCloud.

Vanligt förekommande tjänster i skolorna är möjligheten att via skolans webbplats få åtkomst till bl.a. schema, skolresultat och funktioner för frånvaroanmälan.

En del lärare kommunicerar med elever via sociala medier. Detta är vanligare i gymnasieskolan än i grundskolan. Fyra av tio lärare i gymnasieskolan använder sociala medier för att kommunicera med elever, medan motsvarande i grundskolan är två av tio lärare. I grundskolan är det dock vanligare att lärare i de högre årskurserna använder sociala medier för kommunikation med elever jämfört med lärare i de lägre årkurserna.

Skolverkets undersökning visar sammantaget att digitaliseringen av skolan är relativt långt kommen i Sverige, även med internationella mått mätt.[3]

Det görs dessutom satsningar för att ytterligare påskynda digitaliseringen av skolan, både från kommunalt och statligt håll. Vid Sveriges kommuner och landsting fanns fram till slutet av år 2015 ett s.k. *Nationellt forum för skolans digitalisering* som var en brett sammansatt grupp som arbetade för att underlätta digitaliseringen av skolan.

Vidare har Skolverket, på uppdrag av regeringen, tagit fram ett förslag till it-strategi som vänder sig till förskolan, förskoleklassen, fritidshemmet och den obligatoriska skolan.[4] Skolverket föreslår att det ska vara en vision att skolväsendet präglas av att digitaliseringens möjligheter tas tillvara, så att de digitala verktygen och resurserna

[2] Skolverkets rapport *IT-användning och IT-kompetens i skolan, Skolverkets IT-uppföljning 2015*, dnr 2015:00067.

[3] Se även Digitaliseringskommissionens delbetänkande *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår,* SOU 2014:13, s. 129 f.

[4] *Redovisning av uppdraget om att föreslå nationella IT-strategier för skolväsendet*, Skolverkets redovisning den 4 april 2016 av regeringsuppdrag, dnr 2015:01153.

bidrar till att resultaten förbättras och verksamheten effektiviseras. Enligt förslaget behöver lärarna enkelt kunna samla in uppgifter om elever som genereras när dessa arbetar med digitala läromedel, digitala prov, resultat från nationella prov, bedömningsunderlag och motsvarande. Förhoppningen är att uppgifterna ska underlätta för läraren att individualisera undervisningen och ge eleven underlag för reflektion kring det egna lärandet. Skolverket lyfter också fram att samlandet av uppgifter långt ifrån är problemfritt och att det särskilt reser frågor som har med personlig integritet att göra. Hur uppgifter av detta slag ska hanteras när det gäller skydd av integritet, lagring och åtkomst kommer enligt Skolverket att behöva lösas samlat på nationell nivå. I förslaget sägs också att skolorna står inför ett växande behov att skydda elevernas integritet, samtidigt som man bör använda uppgifterna till att individualisera lärandet, främja forskning och tydliggöra elevens utbildningsframgångar för föräldrar och lärare.

Mot bakgrund av den tilltagande digitaliseringen av skolan och ambitionerna att ytterligare påskynda densamma, är det några resultat i Skolverkets uppföljning som är särskilt värda att notera ur ett integritetsskyddsperspektiv:

- De ökade satsningarna på it i skolan har av undersökningen att döma, inte lett till en lika stor ökning av övergripande styrning och planering. Undersökningen år 2012 visade att färre grundskolor hade en it-plan jämfört med 2008. År 2015 har antalet grundskolor med it-plan ökat och är nu ungefär på samma nivå som 2008. Av alla grundskolor har nu 60 procent en it-plan. Av gymnasieskolorna har 67 procent en it-plan. Av de skolor som har en it-plan, anger 51 procent av grundskolorna och 56 procent av gymnasieskolorna att det i it-planen beskrivs hur skolan ska beakta och hantera elevers integritet i olika it-verktyg och plattformar.
- Omkring fyra av tio lärare uppger att de inte alls arbetar med sina elever för att främja en säker användning av internet (t.ex. gällande utlämnande av personliga uppgifter, bilder, köp av tjänster och varor), och inte heller arbetar något med att förebygga olika former av kränkningar via mobiltelefon och internet.
- Omkring hälften av lärarna i grundskolan anser sig ha ett stort behov av kompetensutveckling inom olika it-områden:

– 55 procent av grundskolelärarna anser att de har ett stort behov av kompetensutveckling beträffande hur man ska arbeta förebyggande mot kränkningar.

– 51 procent av grundskolelärarna anser sig ha ett stort behov av mer kunskap om säker it-användning, och

– 47 procent av grundskolelärarna anser sig ha ett stort behov av kunskap om ”lag och rätt” gällande it-användning.[5]

Intressant ur integritetsskyddsperspektiv är även en rapport från Sveriges kommuner och landsting om rektorers bedömningar i självskattningsverktyget LIKA.[6]

- För 16 procent av skolorna som hade använt sig av LIKA-verktyget gjordes bedömningen att skolan när det gäller digitala verktyg saknade god beställarkompetens och ett bra samarbete med leverantörer om vad skolan behöver. För 48 procent av skolorna gjordes bedömningen att beställarkompetens och bra samarbeta var något som hade påbörjats eller nästan uppnåtts. Övriga bedömde att detta redan uppnåtts.
- För 19 procent av skolorna som hade använt sig av verktyget gjordes bedömningen att skolan när det gäller digitala verktyg saknade tydliggjorda centrala riktlinjer eller rutiner för hur it-relaterade projekt ska redogöras, vem som ansvarar för vad och hur processen går till vid inköp och beställningar. För 46 procent av skolorna gjordes bedömningen att tydliga riktlinjer eller rutiner var något som hade påbörjats eller nästan uppnåtts. Övriga bedömde att detta redan uppnåtts.

Även från statligt håll visar man, som redan nämnts ovan, intresse för skolans digitalisering. Ett aktuellt betänkande som bland annat rör skolans digitalisering är *En digital agenda i människans tjänst – en ljusnande framtid kan bli vår*.[7] Betänkandet är en del av Digitali-

[5] Gymnasielärarna ligger mellan 3 och 6 procent lägre i sina uppskattningar av behovet av kompetensutveckling på samma områden.

[6] Rapporten *Skolans digitalisering – Hur långt har vi kommit?*, Sveriges Kommuner och Landsting, september 2015. LIKA har tagits fram av SKL och är ett nätbaserat självvärderingsverktyg för utvärdering och utveckling av skolans digitalisering. LIKA står för Ledning, Infrastruktur, Kompetens och Användning. Rapporten baserar sig på de självskattningar som i augusti 2015 hade gjorts i LIKA för 873 skolor.

[7] SOU 2014:13.

seringskommissionens uppdrag att verka för att målet i regeringens it-politiska strategi *It i människans tjänst – en digital agenda för Sverige* uppnås.

I betänkandet föreslås en rad åtgärder som syftar till att främja skolans digitalisering. I korthet innebär förslagen ett tydliggörande av digitala hjälpmedels roll i läroplaner och kursplaner, insatser för att höja it-kompetensen hos skolans personal samt åtgärder för bättre kunskap om effekterna av skolans it-användning.

Det är enligt vår uppfattning anmärkningsvärt att när personlig integritet nämns i betänkandet, avses – liksom i många andra sammanhang som rör skolans digitalisering – endast kränkningar på internet, dvs. behovet av att skydda elever från att bli kränkta på internet av andra elever eller av vuxna. Det berörs inte alls i betänkandet att digitaliseringen av skolan medför en ofantlig ökning av möjligheterna för företag, organisationer och myndigheter att kartlägga eleverna.

I sitt remissvar på betänkandet påpekar Datainspektionen att det är viktigt att regeringen i det fortsatta arbetet med utredningens förslag noggrant analyserar vilka konsekvenser behandlingen av personuppgifter har för den enskildes personliga integritet. Datainspektionen lyfter bl.a. fram sin erfarenhet att kunskapen inom skolväsendet om hur personuppgifter får behandlas ofta är bristfällig, och pekar på att det är av central betydelse att kunskap om gällande integritetsskyddslagstiftning också måste finnas hos skolhuvudmännen, dvs. inte bara hos enskilda lärare och rektorer.

7.1.2 Regelverk och tillsyn

Hanteringen av personuppgifter inom utbildningsväsendet regleras av olika författningar, i huvudsak i enlighet med följande:

- Personuppgiftslagen (1998:204). Här kan nämnas att skolornas utbildningsverksamhet anses vara en sådan ”arbetsuppgift av allmänt intresse” som enligt 10 § personuppgiftslagen möjliggör att personuppgifter får behandlas utan den enskildes samtycke.[8]

[8] Se bl.a. Utredningens om offentlighet och sekretess i skolan betänkande *Sekretess i elevernas intresse – Dokumentation, samverkan och integritet i skolan*, SOU 2003: 103 s. 199. Särskilda krav gäller emellertid när det är fråga om känsliga uppgifter i personuppgiftslagens mening, uppgifter om lagöverträdelser eller personnummer.

- Generellt inom offentlig verksamhet gäller offentlighets- och sekretesslagen (2009:400). För fristående skolor finns motsvarande bestämmelser i 29 kap. 14 § skollagen (2010:800). Det bör dock noteras att den mest grundläggande delen av skolverksamheten över huvud taget inte omfattas av offentlighets- och sekretesslagens bestämmelser (eller av motsvande bestämmelser i skollagen). Det är den normala dagliga pedagogiska verksamheten – dvs. den vanliga undervisningen – som inte alls är underkastad sekretess. Uppgifter som rör elevers studieresultat, närvaro och scheman m.m. är med andra ord i princip alltid offentliga. Det är först när verksamheten inriktas på andra åtgärder för elever, t.ex. hälsoundersökningar eller som ett led i s.k. särskild elevstödjande verksamhet, som uppgifter av hänsyn till elevernas och deras närståendes integritet kan vara sekretessbelagda.[9]
- Skollagen.
- Patientdatalagen (2008:355) gäller för den hälso- och sjukvård som bedrivs på skolorna. För uppgifter i hälso- och sjukvården i skolorna gäller offentlighets- och sekretesslagen. För privata vårdgivare som bedriver hälso- och sjukvård i skolan finns motsvarande bestämmelser i patientsäkerhetslagen (2010:659).

I första hand följande tillsynsmyndigheter kontrollerar hanteringen av personuppgifter inom utbildningsväsendet: Datainspektionen (utövar tillsyn enligt personuppgiftslagen), Skolinspektionen (utövar tillsyn enligt skollagen), Barn- och elevombudet (som är en del av Skolinspektionen och bl.a. kan begära skadestånd för barn och elever som varit utsatta för kränkningar i skolan), Inspektionen för vård och omsorg (utövar tillsyn enligt hälso- och sjukvårdslagstiftningen med inriktning på patientsäkerhet inom skolhälsovården).

Därtill utövar Riksdagens ombudsmän (Justitieombudsmannen) och i viss mån Justitiekanslern tillsyn över det allmänna utbildningsväsendet.

[9] SOU 2003:103, s. 65 f. I ett senare betänkande, Utredningens om sekretess för uppgifter i skolväsendet och vissa andra utbildningsformer och verksamheter betänkande *Skolans dokument – insyn och sekretess*, SOU 2011:58, har vissa ändringar föreslagits, bl.a. att individuella utvecklingsplaner skulle omfattas av sekretess, men förslagen har inte lett till lagstiftning.

Den enskilde som anser att hennes eller hans uppgifter hanterats på ett felaktigt sätt, kan således vända sig till olika tillsynsmyndigheter med ett klagomål. Beroende på vad klagomålet rör, är det olika myndigheter som ansvarar för tillsynen. Exempelvis ansvarar Datainspektionen för frågor som rör vilka uppgifter om eleverna som får hanteras och hur länge de får sparas. Skolinspektionen ansvarar för frågor som rör hur skolorna dokumenterar elevernas arbete. Barn- och elevombudet kan i tvister om skadestånd enligt skollagens sjätte kapitel (med förbud mot kränkande behandling) föra talan för en elev som samtycker till det. Inspektionen för vård och omsorg ansvarar t.ex. för frågor om tillsyn av om dokumentationen uppfyller patientdatalagens krav.

Vidare finns det en möjlighet för eleven att själv begära skadestånd för den ideella skada (dvs. kränkningen) som hon eller han anser sig ha lidit på grund av integritetsintrång, och att i så fall väcka talan vid allmän domstol.

7.2 Digitala lärplattformar och läromedel

7.2.1 Företeelserna

Digitala lärplattformar

Digitala lärplattformar är internetbaserade system som möjliggör olika sorters interaktivitet och kommunikation mellan elever, lärare och vårdnadshavare. Den vanliga engelska beteckningen för dem är *Learning Management Systems* (LMS).

De digitala lärplattformarna kallas ibland för virtuella klassrum, och innehåller vanligen funktioner för:

- att skapa grupper och klasser,
- att visa schema och närvaro eller frånvaro,
- att visa betyg, omdömen och individuella utvecklingsplaner,
- att genomföra prov,
- diskussionsforum och chattfunktion,

- virtuella rum där lärare och elever kan skicka meddelanden och läraren kan lägga ut planering, undervisningsmaterial, länkar osv. och eleverna kan lösa och lämna in uppgifter, och
- åtkomst för vårdnadshavare för att kunna kommunicera med skolan och följa det egna barnets arbete.

Digitala lärplattformar kan möjliggöra en detaljerad loggning av elevens aktiviteter med information om exempelvis när på dygnet eleven arbetar i systemet, hur eleven arbetar med en viss uppgift, hur eleven interagerar och kommunicerar med lärare och andra elever och hur aktivt eleven arbetar med sina olika ämnen i systemet.

Informationen om elevens aktiviteter i den digitala lärplattformen kan användas för att få veta mer om elevens inlärningsprocesser. Kunskap om elevens inlärning gör det möjligt både att anpassa uppgifter och arbetssätt till den individuella eleven, att identifiera elever som behöver särskilt stöd, och till att allmänt förbättra systemen. Det här området kallas ibland för inlärningsanalys (på engelska *learning analytics*), vilket kan sägas vara en tillämpning av big data-analyser på utbildningsområdet, i vilket uppgifter från lärplattformar är en av flera möjliga datakällor.

Inlärningsanalys är ännu i sin linda, men spås bli viktigt i en nära framtid. Vissa lärplattformar med stor spridning i Sverige förbereder redan i dag sina lärplattformar för att kunna stödja inlärningsanalys.[10]

Ofta finns lärplattformen i molnet. Det är alltså en annan organisation än skolan som lagrar personuppgifterna och står för systemets drift. Det innebär att de frågeställningar som uppkommer för molntjänster är aktuella även för lärplattformarna. Faktum är att de molntjänster som i Sverige granskats mest ingående av Datainspektionen, har varit just lärplattformar Exempelvis har den molnbaserade lärplattformen Google Apps for Education granskats och kritiserats i en rad beslut.

Några exempel på andra i Sverige vanligt förekommande lärplattformar är Fronter, Pingpong och Infomentor. Det är inte ovanligt att mindre lärplattformar delvis är integrerade med andra, större plattformar, som exempelvis nämnda Google Apps for Education.

[10] *Personvern 2015 – tillstand og trender*, rapport från Datatilsynet och Teknologirådet i Norge.

På universitet och högskolor används lärplattformar för s.k. MOOC-kurser (vilket står för *Massive Open Online Course*) som är webbaserade kurser som oftast både är gratis och öppna för allmänheten. MOOC-kurser har i USA uppmärksammats för oklarheter kring vilken lagstiftning som skyddar det stora antal personuppgifter som behandlas om studenterna när de genomgår MOOC-kurser.[11]

Digitala läromedel

Det finns många olika digitala läromedel på marknaden. Ofta handlar det om material som kombinerar text, ljud och bild, som är interaktivt och som är åtkomligt över nätet. Digitala läromedel kan underlätta inlärningen och göra undervisningen effektivare eftersom läraren inte behöver delta i de moment där läromedlet kan instruera eleven. Läraren kan i stället fokusera på de delar som absolut kräver hans eller hennes handledning.

Ofta förutsätter användningen av digitala läromedel att varje enskild elev registreras som användare hos leverantören, dvs. hos förlaget. Leverantören kan då vanligen följa elevens användning av läromedlet på en mycket detaljerad nivå. Även data från elevernas användning av läromedel är förstås av stort intresse för inlärningsanalys.

Digitala läromedel ges i Sverige ut av förlag som även ger ut pappersbaserade läroböcker och av förlag som enbart sysslar med digitala läromedel.

7.2.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter i digitala lärplattformar och läromedel. Av särskild betydelse är i detta sammanhang är personuppgiftslagens bestämmelser om personuppgiftsansvaret, ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

[11] Steve Kolowich, *Are MOOC-Takers 'Students'? Not When It Comes to the Feds Protecting Their Data*, publicerad den 3 december 2014 i The Chronicle of Higher Education.

7.2.3 Risker för den personliga integriteten

När alla funktioner i digitala lärplattformar och läromedel används av eleverna, genereras en stor mängd mycket detaljerade uppgifter om vad de arbetar med, hur de arbetar och om deras relationer till andra elever och till lärare.

Det generella gapet mellan det formella ansvaret för hanteringen av personuppgifterna och kunskapen och kontrollen över hur uppgifterna faktiskt hanteras, medför förstås en rad olika risker ur ett integritetsskyddsperspektiv.

Det finns en risk för att onödigt många uppgifter om eleverna hanteras i systemen och för att uppgifterna sprids och hanteras för andra ändamål än de som huvudmannen ursprungligen bestämt och informerat elever och vårdnadshavare om. Det strider i så fall mot personuppgiftslagen och kanske även mot de avtal som finns mellan huvudmanen och personuppgiftsbiträdena.

En faktor som driver på och ökar dessa risker är det stora intresset hos leverantörer, systemutvecklare och förlag av att hantera så många olika uppgifter som möjligt från de digitala lärplattformarna och läromedlen. Syftet med det är att kunna använda inlärningsanalytiska metoder för att utveckla och förbättra system och läromedel. Här är verkligen *alla* uppgifter som över huvud taget kan lagras av intresse, även innehållet i chattar mellan eleverna och likaså samtal i den mån ljud lagras i systemet och kan analyseras (jfr s.k. *social metrics*).

Skolverket är medvetet om utvecklingen och skriver följande på sin webbsida.

> Under de senaste åren har möjligheterna att göra detta [samla kunskap om elevernas sätt att lära] med digitalt stöd ökat till exempel genom användningen av lärplattformar och verktyg för individuella utvecklingsplaner. Samtidigt som vi ser hur den tekniska utvecklingen kraftigt ökar möjligheterna för att samla data aktualiseras frågor om vad som är önskvärt och lämpligt.[12]

[12] *Samla och analysera*. Skolverket. http://www.skolverket.se/skolutveckling/resurser-for-larande/itiskolan/digitala-larresurser/learning-analytics-1.223404 Hämtat 2016-05-09.

Om det finns brister i huvudmännens kunskap om, och kontroll över hur uppgifter hanteras i lärplattformarna, finns det naturligtvis också en stor risk för att elever och vårdnadshavarna varken får tillräcklig information om hanteringen eller får möjlighet att påverka hanteringen.

Vissa av de största och mest populära lärplattformarna i molnet är ”gratis” för skolan, på så sätt att någon direkt ekonomisk ersättning inte begärs för tjänsterna. I den rådande affärsmodellen får dock leverantörerna sin ersättning i form av användbara uppgifter om de elever vars uppgifter hanteras i systemen, som leverantörerna driftar för skolhuvudmannans räkning.

Digitala lärplattformar hämtar vanligen grunduppgifter om eleverna från något av skolhuvudmannens elevregister. Dessa kan vara rent administrativa databaser eller kommungemensamma befolkningsregister. Det finns då en risk för att det förs över fler uppgifter än vad lärplattformen egentligen behöver. Det finns också en risk för att uppgifter om elever med skyddad identitet förs över och får en spridning i lärplattformen som innebär att personernas identiteter röjs.

7.3 Sociala medier i undervisningen

7.3.1 Företeelsen

Sociala medier är ett sätt att kommunicera, skapa relationer, främja dialog och dela kunskap. Exempel på sociala medier är:

- webbplatser med nyhetskommentarer, länkar, chatt och kommentarsfält,
- Facebook, LinkedIn, Twitter, YouTube, Flickr och många andra,
- bloggar, och
- wikier, där användarna hjälps åt att skapa innehållet.[13]

Under senare år har det blivit populärt att använda sociala medier i skolan, som ett inslag i undervisningen eller som ett sätt att hålla kontakt lärare emellan. Sociala medier är snabba, lättanvända och gör det enklare att omvärldsbevaka, kommunicera och dela material med

[13] E-delegationens riktlinjer *Myndigheters användning av sociala medier*, version 1.0, 2010-12-30.

elever, föräldrar och kollegor. Vissa lärare menar att deras elever blir motiverade att skriva och skapa när deras material blir synligt för en vidare krets än klasskamraterna. Andra lyfter fram betydelsen av att lärarna får ett stort professionellt nätverk för kollegialt lärande och diskussion.

Facebook, bloggar och wikier[14] är populära redskap i skolan för samarbete, kommunikation och publicering av text, bild och ljudfiler.

7.3.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter i sociala medier. Av särskild betydelse i detta sammanhang är personuppgiftslagens bestämmelser om personuppgiftsansvaret, ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

Ibland krävs samtycke för att hanteringen ska vara förenlig med personuppgiftslagen, exempelvis vid ingående av avtal med det sociala mediet om personuppgiftshanteringen. Av betydelse är då att personuppgiftslagen saknar bestämmelser om från vilken ålder unga personer själva kan samtycka till att uppgifterna publiceras. Datainspektionen anger följande i frågan:

> Också den som är underårig (det vill säga under 18 år) kan lämna giltigt samtycke till en tilltänkt behandling om han eller hon är kapabel att förstå innebörden av samtycket. (…) Om uppgifter om underåriga ska behandlas är det särskilt viktigt att göra en seriös bedömning av den unges förmåga att förstå de totala konsekvenserna av en behandling. En tumregel kan vara att den som fyllt 15 år normalt är kapabel att ta ställning i samtyckesfrågan. Många gånger är det dock så att andra regler än de som finns i personuppgiftslagen hindrar att personuppgifter om barn behandlas. Det finns till exempel begränsningar när det gäller att skicka direktreklam till barn.[15]

Här kan också föräldrabalkens bestämmelser om möjligheten att ingå avtal med underåriga bli tillämpliga.

I Konsumentverkets Vägledning om marknadsföring riktad till barn och unga, berörs möjligheten att ingå avtal med underåriga:

[14] En wiki är en webbplats där besökarna själva skapar innehållet, ett känt exempel är Wikipedia.
[15] Datainspektionens informationsskrift *Samtycke enligt personuppgiftslagen*. Se även Artikel 29-gruppens yttrande 1/2008 *on the protection of children's personal data (General guidelines and the special case of schools)*.

> Barns behörighet att ingå avtal regleras i föräldrabalkens 9 kap. Den som är under 18 år är omyndig och får inte själv ingå avtal. Barn som fyllt 16 år får dock själva bestämma över pengar som de tjänat. Avtalsparten måste i varje enskilt fall ta reda på om den andra avtalsparten är myndig och behörig att ingå avtal. Det räcker alltså inte med att ett företag tror att motparten är myndig för att ett avtal ska bli giltigt. För att ett avtal med en minderårig ska bli giltigt krävs att förmyndare, normalt föräldern, samtyckt till det.

I vägledningen berörs emellertid varken personuppgiftslagen eller avtal som reglerar just hanteringen av personuppgifter.

I Frankrike har konsumentskyddsmyndigheten Commission des clauses abusives år 2014 formulerat rekommendationer för hur sociala medier bör utforma sina avtalsvillkor. Flera av rekommendationerna rör avtalsvillkor om hanteringen av personuppgifter. Myndigheten pekar inledningsvis på problemet att sociala medier vanligen felaktigen utgår från att underåriga har sina legala ställföreträdares godkännande till att ingå avtal med det sociala mediet. Därefter rekommenderar myndigheten att sociala mediers avtalsvillkor ska föreskriva uttryckligt samtycke från den underåriges legala ställföreträdare beträffande behandlingen av uppgifter om underåriga som saknar kapacitet att själva lämna ett giltigt samtycke.[16]

Det finns inga motsvarande rekommendationer om sociala mediers avtalsvillkor om personuppgifter från det svenska Konsumentverket.

7.3.3 Risker för den personliga integriteten

I kommitténs kontakter med skolföreträdare har framförts att användningen av sociala medier i undervisningen kan medföra många fördelar för eleverna, exempelvis att elever kan uppleva det som stimulerande och positivt när deras skolarbeten kan ses av en större publik på sociala medier. Samtidigt innebär de sociala mediernas hantering av uppgifter om eleverna en rad olika risker ur ett integritetsperspektiv.

Sociala medier kan även användas av elever för att sprida kränkande uppgifter om andra. Nya skyddsintressen har därför uppkommit och medfört ett väsentligt ökat behov av ett bättre utformat straffrättsligt skydd för privatlivet och den personliga integriteten.

[16] *Recommandation n°2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux* http://www.clauses-abusives.fr/recom/index.htm Hämtat 2016-05-09.

Med den motiveringen föreslås i betänkandet *Integritet och straffskydd*[17] en ny straffbestämmelse om s.k. olaga integritetsintrång som tar sikte på kränkningar som enskilda personer begår mot andra enskilda. Eftersom detta område nyligen varit föremål för en grundlig granskning och analys, avstår vi från att undersöka det.

Generella risker

Användning av sociala medier i skolan medför, liksom användning av sociala medier på andra områden, vissa generella risker.

Uppgifter om elever kan komma att spridas och hanteras för ändamål som eleverna eller deras vårdnadshavare inte känner till eller har samtyckt till. Det sociala mediet kan exempelvis skanna av material för att kunna meddela upphovsrättsinnehavare om möjliga intrång i upphovsrätten (såsom otillåten spridning), eller ge okända tredjepartsapplikationer åtkomst till uppgifter eller av misstag publicera uppgifter öppet på internet.

Sammanblandning med elevernas privatliv

Om skolan använder sig av sociala medier i undervisningen, kan det innebära att den, med stöd av skolplikten, mer eller mindre tvingar elever att skaffa sig personliga konton i sociala medier. För många elever är detta inget problem eftersom de redan själva valt att skaffa eget konto och att vara aktiva. Kunskaper om sociala medier hör också till det som skolan förväntas lära ut till eleverna. Men vissa elever skulle kanske inte själva välja just det sociala mediet som skolan använder sig av, eller så skulle de kanske välja att inte alls vara aktiva på något socialt medium överhuvudtaget.

I skolmiljö är det också ett omtalat problem att användning av sociala medier i undervisningen innebär att eleverna förutsätts ingå egna, individuella avtal med de sociala medierna, i stället för att exempelvis ansluta sig till ett gruppkonto eller en gruppinloggning som delas av hela klassen. Om eleven redan har ett personligt konto, blandas elevens privata förehavanden på mediet med det eleven gör på

[17] Utredningens om ett modernt och starkt straffrättsligt skydd för den personliga integriteten betänkande *Integritet och straffskydd*, SOU 2016:7.

mediet som ett led i undervisningen. Företaget som tillhandahåller det sociala mediet kommer då enkelt att kunna använda sig av både privata och skolrelaterade uppgifter om eleven för att genomföra en så detaljerad profilering som möjligt.

Sociala medier i molnet

Datainspektionen har i ett ärende granskat en skolas användning av bloggar.[18] Varje klass i skolan hade en egen blogg, med syftet att informera och kommunicera med elever och vårdnadshavare. Eleverna kunde med hjälp av bloggarna visa egna arbeten och se vad kamraterna på skolan arbetade med. Inläggen i bloggarna skrevs av eleverna på lektionstid. De personuppgifter som normalt publicerades var förnamn och bild, och lärarna modererade kommentarer i bloggarna. Datainspektionen hade inga invändningar mot bloggarna när de användes för att informera och kommunicera med elever och vårdnadshavare. Tvärtom uttalade Datainspektionen att

> Det finns många positiva aspekter av att låta elever arbeta med sociala medier i skolan. Under överinseende av ansvariga lärare kan eleverna exempelvis få möjlighet att lära sig använda webbverktyg som tillhandahålls via internet och parallellt föra en dialog om vad som är viktigt att tänka på när information publiceras på internet och vilka konsekvenser en otillåten eller olämplig publicering kan få.

Datainspektionen lyfte emellertid fram att bloggar vanligen är molnbaserade och att det därmed uppstår särskilda skyldigheter för den personuppgiftsansvarige skolhuvudmannen, som i detta fall var Kunskapsnämnden i kommunen.[19] I så fall måste nämnden ha regler för vilka personuppgifter som är tillåtna att publicera. En förutsättning för att reglerna ska få nödvändigt genomslag i organisationen är enligt Datainspektionen att de regelbundet kommuniceras och diskuteras med ansvariga lärare och elever. Slutligen pekade Datainspektionen på att all skolverksamhet måste se till att elever som lever med skyddade personuppgifter skyddas på ett adekvat sätt.

[18] Datainspektionens dnr 1707-2013.

[19] I ärendet hade skolan i samband med Datainspektionens tillsyn slutat använda bloggarna, vilket kan vara anledningen till att Datainspektionen inte ställde frågan om bloggen i fråga verkligen var molnbaserad.

Skolan använde sig även av en enkätfunktion som fanns inbyggd i bloggen. I enkäterna ställde skolan frågor bl.a. om eleverna hade kompisar på rasterna och om de kände sig trygga på skolans toaletter, samt om en rad mindre känsliga ämnen. Eleverna kunde också svara på frågor i fritextfält, och där själva komma in på andra känsliga ämnen. Enkäterna och elevernas svar lagrades i bloggens enkätfunktion. Datainspektionen konstaterade att det rörde sig om integritetskänsliga uppgifter som hanterades i enkäterna, och att det medförde ett krav på bättre skydd (kryptering och stark autentisering) för personuppgifterna är vad som faktiskt användes i bloggen. Därutöver kom Datainspektionen åter in på den omständigheten att bloggar vanligen lagras och behandlas i molnet. Eftersom de personuppgiftsansvariga normalt sett saknar insyn och kontroll över uppgifter som hanteras i molnet framhöll Datainspektionen att det under alla omständigheter var olämpligt att behandla känsliga eller integritetskänsliga personuppgifter i skolbloggar och enkätverktyg.

Liksom för molntjänster generellt (se kapitel 21 om molntjänster) finns det en risk med molnbaserade social medier att de enskilda inte kan få information om vem som faktiskt hanterar deras uppgifter och vilka uppgifter dessa okända personuppgiftsansvariga får åtkomst till. Det kan också förekomma att uppgifter om enskilda användare sprids till underleverantörer utanför EES i länder med en dataskyddsreglering som inte når upp till en tillfredsställande skyddsnivå.

7.4 Elevhälsan

7.4.1 Företeelsen

I och med att skollagen började tillämpas den 1 juli 2011 samlades skolhälsovården, den särskilda elevvården och de specialpedagogiska insatserna i en samlad elevhälsa. Elevhälsan omfattar medicinska, psykologiska, psykosociala och specialpedagogiska insatser. Syftet med att samla insatserna var bland annat att öka samverkan och att betona det hälsofrämjande och förebyggande arbetet. Elevhälsans mål är att skapa en så positiv lärandesituation som möjligt för eleven.[20]

[20] Socialstyrelsens och Skolverkets *Vägledning för elevhälsan*, oktober 2014.

Elevhälsans arbete kräver ofta att personalen har ett fungerande informationsutbyte med annan personal på skolan, liksom externt med till exempel hälso- och sjukvården och socialtjänsten.

7.4.2 Det skyddande regelverket

Patientdatalagens bestämmelser gäller för den verksamhet inom elevhälsan som handlar om dokumentation av hälso- och sjukvård.

För skolor som bedrivs i det offentligas regi gäller offentlighets- och sekretesslagen. För friskolor finns motsvarande bestämmelser om tystnadsplikt i 29 kap. 14 § skollagen.

Varje kommunal nämnd som bedriver utbildning är en egen myndighet. Personal inom en och samma myndighet kan lämna sekretessbelagda uppgifter mellan sig om det behövs för att handlägga ett ärende eller bedriva verksamheten. Om det finns självständiga verksamhetsgrenar inom en myndighet gäller dock sekretess mellan de olika verksamheterna. Inom skolan är den medicinska insatsen inom elevhälsan en självständig verksamhetsgren. Det innebär att sekretess gäller för uppgifter i elevhälsans medicinska insats och att en sekretessprövning måste göras om man vill lämna ut uppgifter till elevhälsans övriga delar eller till övrig personal inom skolan.

För skolläkare och skolsköterskor gäller samma sekretess som för annan hälso- och sjukvårdspersonal. Detta innebär att det finns en sekretessgräns gentemot övrig skolpersonal. Uppgifter om en enskild elev får dock lämnas från elevhälsans medicinska insatser till rektorn, någon annan inom elevhälsan eller en särskild elevstödjande verksamhet inom samma kommunala nämnd, om det krävs för att eleven ska få nödvändigt stöd. Bestämmelsen ska dock tillämpas restriktivt och i första hand ska samtycke inhämtas. I de sällsynta undantagsfall som bestämmelsen är avsedd för måste elevens rätt till utbildning och behov av särskilt stöd kunna ges företräde framför skyddet för elevens integritet som patient.[21]

[21] Socialstyrelsens och Skolverkets *Vägledning för elevhälsan*, oktober 2014.

7.4.3 Risker för den personliga integriteten

Det ställs långtgående krav på skolorna att de ska dokumentera sin verksamhet och sina insatser för enskilda elever, inte minst på elevhälsans område. Det innebär att det kan hanteras mycket känsliga uppgifter om eleverna i skolorna.

Samtidigt ställs också långtgående krav på samverkan mellan olika yrkeskategorier i skolan för att tillsammans uppnå god hälsa för eleverna, vilket kan innebära ett krav på spridning av känsliga uppgifter.

Likaså finns det ett detaljerat regelverk för sekretess och personuppgiftsbehandling inom elevhälsan och särskilt inom den hälso- och sjukvård som bedrivs inom ramen för elevhälsan.

Det kan rimligen antas att det i den dagliga verksamheten på skolorna uppstår svåra frågor om tillämpningen av regelverket angående hur olika befattningshavare får dela information om eleverna med varandra.

Det saknas emellertid undersökningar ur ett integritetsskyddsperspektiv från senare år om hur personuppgifter från eller inom elevhälsan hanteras i skolorna.

Det förefaller inte osannolikt att området på grund av sitt relativt komplexa regelverk tillsammans med kraven på samarbete, kräver kontinuerliga kunskapshöjande insatser för berörd personal på skolorna.

Skolinspektionen avslutade år 2015 ett tillsynsprojekt inom vilket man granskade på elevhälsans arbete för att motverka risker för att elever ska hamna i psykisk ohälsa. Tillsynens fokus låg således inte på sekretess och integritetsskydd, även om det i granskningsrapporten poängteras att eleverna behöver kunna känna sig säkra på att förtroende och sekretess respekteras.[22]

Skolinspektionens erfarenheter från tidigare tillsynsaktiviteter på området har varit att olika befattningshavare i skolan samverkar för litet i arbetet för att främja elevernas hälsa.[23]

[22] Skolinspektionens rapport 2015:05, *Elevhälsa – Elevers behov och skolans insatser*.
[23] Se Skolinspektionens kunskapsöversikt för kvalitetsgranskning av elevhälsans arbete med dnr 2014:2123.

7.5 Skolfederationen

7.5.1 Företeelsen

Ett intressant initiativ för att möta digitaliseringen av skolan, är i Sverige den s.k. Skolfederationen. Skolfederationen är en identitetsfederation, dvs. en samarbetsform där tanken är att de samverkande parterna ska lita på varandras användaridentifiering.

Skolfederationen har tagits fram under ledning av SIS, Swedish Standards Institute, och drivs av IIS (Internetstiftelsen).

Nyttan med Skolfederationen ligger i att alla olika IKT-tjänster som används i en skola och som har olika leverantörer, ska presenteras i ett och samma konto för eleven. Eleven ska därmed bara behöva ett användarnamn och ett lösenord för åtkomst till samtliga tjänster.

Skolfederationen beskriver på sin webbsida den typiskt förekommande situationen i skolan i dag när man inte tillämpar någon federativ identitetslösning. I en skola kan finnas externt driftade tjänster för digital lärplattform, system för schemaläggning och frånvarorapportering, digitala läromedel, media/streamingtjänster och bloggportaler. I dagsläget, utan någon federativ identitetslösning, har alla externa tjänster sin egen kontohantering. En elev behöver alltså hålla reda på användarnamn och lösenord för ett flertal personliga konton och klasskonton. Det medför en risk för att eleverna ska glömma sina lösenord och få problem med inloggningen. Om skolan och tjänsteleverantörerna är anslutna till Skolfederationen samlar man allt till ett konto per elev.

Syftet med Skolfederationen är således att underlätta elevernas och skolornas användning av digitala tjänster och läromedel.

I syfte att kunna minimera exponeringen av personuppgifter, finns det inom Skolfederationen en möjlighet för skolhuvudmännen att bestämma hur många och vilka uppgifter om eleverna som ska visas för andra aktörer som är anslutna till Skolfederationen. Utgångspunkten är att det i normalfallet inte ska vara möjligt för andra anslutna aktörer att överhuvudtaget identifiera enskilda elever.

7.5.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter i Skolfederationen. Av särskild betydelse är i detta sammanhang är personuppgiftslagens bestämmelser om personuppgiftsansvarets placering och omfattning, om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

7.5.3 Risker för den personliga integriteten

Skolfederationen är ett intressant exempel eftersom den kan ge ett förbättrat integritetsskydd för eleverna samtidigt som den också underlättar skolsektorns hantering av elevernas personuppgifter.

Skolfederationen omfattar i dag många av Sveriges elever i grund- och gymnasieskolan. Skolfederationen har dock inte granskats av Datainspektionen ur ett integritetsskyddsperspektiv.

En risk som kan uppstå vid en anslutning till Skolfederationen är att skolhuvudmännen av misstag eller okunskap kan välja en nivå för kommunikationen där integritetskänsliga uppgifter om enskilda elever onödigtvis visas för anslutna aktörer, dvs. att integritetskänsliga uppgifter får en större spridning av än vad som är fallet utan federativ identitetslösning.

En annan risk är att vissa integritetsskyddande åtgärder, rörande exempelvis gallring av uppgifter som inte längre behövs eller skyddet för personuppgifterna (informationssäkerheten), generellt sett har en benägenhet att falla mellan stolarna i komplexa samarbeten kring personuppgifter och systemintegreringar. Frågan om personuppgiftansvarets placering och omfattning, blir ofta svårare ju fler olika aktörer som blir inblandade i samarbeten av detta slag.

Single-sign-on-lösningar ger åtkomst till flera system med hjälp av en och samma inloggning. De anses därmed rent generellt innebära en risk för den personliga integriteten, eftersom de kan innebära att ett stort antal uppgifter blir tillgängliga genom en inloggning.

Det bör samtidigt noteras att en genomtänkt användning av Skolfederationen (liksom av andra federativa lösningar där medverkande organisationer litar på varandras användaridentifiering) kan skapa bättre förutsättningar för utveckling av gemensamma principer och praxis kring gallring och skydd för personuppgifterna än vad som har varit fallet tidigare.

7.6 Kameraövervakning i skolor

7.6.1 Företeelsen

Kameraövervakning är sedan några år tillbaka relativt vanligt förekommande i skolor.

Det finns både kameror som övervakar området utomhus utanför skolbyggnaden och kameror som övervakar det inre av skolbyggnaderna. Det saknas aktuella uppgifter om hur många skolor som har någon form av kameraövervakning.

År 2008 redovisade Datainspektionen en undersökning som visade att antalet skolor som använde kameraövervakning då hade ökat med över 150 procent jämfört med år 2005. Enligt enkätsvaren år 2008 använde mer än var femte skola kameraövervakning. Av de skolor som ännu inte hade börjat med kameraövervakning övervägde mer än var femte att installera kameror.[24]

Vanliga skäl till att vilja införa kameraövervakning inomhus i skolan är stölder från elevskåp eller skadegörelse och klotter.

Utanför skolan är skadegörelse på skolans egendom ett vanligt skäl till att införa kameraövervakning. Ofta görs sådan övervakning utanför ordinarie skoltider, dvs. på kvällar, nätter och helger då risken för skadegörelse anses vara högst.

Enligt Brottförebyggande rådet saknas det svenska utvärderingar av kameraövervakningens brottsförebyggande effekt i skolor.

7.6.2 Det skyddande regelverket

Kameraövervakningslagen (2013:460) gäller oavsett om allmänheten har tillträde till den övervakade platsen eller inte. Huvudregeln är att det krävs tillstånd för kameraövervakning av platser dit allmänheten har tillträde, men ibland räcker det med endast en anmälan.

Den som planerar att bedriva kameraövervakning av platser dit allmänheten inte har tillträde behöver inget tillstånd. Men övervakningen måste följa kameraövervakningslagens bestämmelser. Lagen ger två möjligheter: Den ena är att den som ska övervakas lämnar sitt samtycke till övervakningen. Den andra möjligheten är att

[24] *Kameraövervakning på skolor ökar med över 150 procent*. Datainspektionen, 2008. http://www.datainspektionen.se/press/nyheter/2008/kameraovervakning-pa-skolor-okar-med-over-150-procent/ Hämtat 2016-05-09.

övervakningen görs efter att man tillämpat överviktsprincipen, vilken innebär att kameraövervakningen är tillåten om övervakningsintresset väger tyngre än den enskildes intresse av att inte bli övervakad. Exempel på övervakningsintressen kan vara att förebygga, utreda och avslöja brott och förhindra olyckor.

Lagen innehåller också bestämmelser om hur länge bild och ljud från kameraövervakning får sparas och hur inspelningarna ska skyddas.

Det finns praxis från Högsta förvaltningsdomstolen avseende kameraövervakning i skolor inomhus. Domstolen konstaterade i en dom[25] att kameraövervakning av lektionssalar, korridorer, bibliotek, uppehållsrum och liknande i en skola under skoltid generellt sett måste betraktas som ett intrång i de registrerades integritet. För att en sådan övervakning inte ska vara kränkande i den mening som avses i 5 a § personuppgiftslagen bör det därför enligt domstolen krävas att det i det enskilda fallet står klart att det finns ett påtagligt behov av övervakningen och att detta väger tyngre än den enskildes intresse av att inte bli övervakad. I målet befanns den aktuella kameraövervakningen inte vara förenlig med personuppgiftslagens bestämmelser.

Även om domen meddelades innan den nuvarande kameraövervakningslagen trädde i kraft, kan domstolens ställningstagande fortsatt vara vägledande för hur den numera lagstadgade avvägningen ska göras.

För närvarande pågår en översyn av kameraövervakningslagen i Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd.[26] Utredaren ska enligt direktiven bl.a. ta ställning till om integritetsskyddet på vissa platser dit allmänheten inte har tillträde, till exempel arbetsplatser och skolor, behöver förbättras. Uppdraget ska redovisas senast den 28 februari 2017.

7.6.3 Risker för den personliga integriteten

Många elever vistas i skolan under större delen av dagen. Många har också en stor del av sin umgänges- och vänkrets bland andra elever i samma skola. Därtill kommer att elever i grundskolan har en lag-

[25] HFD 2012 ref. 16.
[26] Ju 2015:14.

stadgad skyldighet att vistas i skolan på grund av skolplikten. Det gör att övervakning av elever inomhus i skolan måste anses som relativt närgången.

Även om det som nämnts saknas aktuella siffor för hur vanlig kameraövervakning i skolorna är i dag, kan på grundval av äldre undersökningar och medieuppgifter antas att det i vart fall rör sig om ett betydande antal skolor i landet som använder sig av kameraövervakning.

Antalet kameror som sitter uppe i skolor där man använder sig av kameraövervakning inomhus, varierar kraftigt mellan skolorna. Även på denna punkt saknas aktuella siffor. Det är dock inte ovanligt med ett relativt stort antal kameror, exempelvis fanns 60 kameror inomhus i det ärende som slutligen avgjordes av Högsta förvaltningsdomstolen, även om ett så stort antal kameror säkerligen hör till ovanligheterna.

I skolor med ett stort antal kameror, kan det vara svårt för eleverna att hitta områden där de inte övervakas. I dessa fall är övervakningen både ingående och omfattande på så vis att många av elevernas vardagssituationer fångas av någon kamera.

Enligt vad kommittén känner till förekommer det inte i dagsläget att någon skola använder sig av samtycke som grund för kameraövervakningen.

Erfarenheten från Datainspektionens tillsyn är att det inte alltid är skolhuvudmannen eller skolledningen som fattar beslutet om att sätta upp kameror och om hur många kameror det ska finnas samt var de ska vara placerade. Dessa beslut kan många gånger i praktiken fattas på en lägre nivå i organisationen, även om beslutsrätten inte delegerats formellt. Besluten ifråga är oftast inte skriftligen dokumenterade.

I en undersökning som Datainspektionen år 2010 lät genomföra om ungdomars inställning till personlig integritet, visade det sig att kameraövervakning generellt sett var den mest accepterade formen av övervakning, men att man däremot inte ville ha övervakningskameror i klassrum och i uppehållsrum i skolan.[27]

[27] Datainspektionens rapport 2011:1 *Ungdomar och integritet 2011.*

7.7 Kommitténs samlade bedömning av området

Av det här kapitlet framgår att det genereras allt fler och allt mer detaljerade uppgifter om eleverna i skolan, alltifrån hur de använder sig av läromedel och chattar med klasskamraterna, till vilka kamrater de helst syns tillsammans med i skolan.

Uppgifterna kan användas på ett sätt som innebär stor nytta för eleverna, t.ex. när de används för att utforma det stöd den enskilde eleven behöver i skolarbetet. Samtidigt finns det ett antal olika risker med den ökande mängden uppgifter om eleverna.

Det mesta av den tilltagande personuppgiftsmassan om eleverna hanteras utan deras eller vårdnadshavarnas samtycke. Det kan också hända att uppgifterna hanteras med stöd av samtycken vars lämplighet eller giltighet kan ifrågasättas.

Det finns oftast tydliga regler om att elever eller vårdnadshavare ska informeras om hanteringen av elevernas uppgifter. Men många gånger har inte ens den ansvarige, dvs. skolhuvudmannen, överblick över vilka uppgifter som hanteras av vem och hur. Den information som sedan ges vidare till elever och vårdnadshavare kan därför ofta antas vara mer eller mindre bristfällig.

De företeelser som nämns i det här kapitlet har inte granskats ur ett integritetsskyddsperspektiv på senare år, förutom när det gäller kameraövervakning och molntjänster. Det finns inte heller någon myndighet eller annan aktör som kan sägas ha en helhetsbild av vad som försiggår med bäring på integritetsskyddet i landets tusentals skolor – i vad mån kameraövervakning används, molntjänster anlitas, vilka sociala medier som används osv.

I sammanhanget är av betydelse att det rör sig om barns rätt till personlig integritet. Barn måste anses som särskilt viktiga när det gäller att skyddas mot otillbörliga intrång i den personliga integriteten, på samma sätt som de anses särskilt skyddsvärda i konsumenträttsliga sammanhang. Barn kan behöva stöd när det gäller att freda sin personliga sfär eller när de behöver fatta beslut som rör deras nutid och framtid.

Ytterligare skäl till att vara särskilt försiktig med en närgången digital kartläggning av barn, är att erfarenheterna från skolan kommer att prägla dem för resten av livet – även när det gäller frågor om

vilka intrång som ska accepteras och vad den enskilde kan förvänta sig att få veta och möjlighet att påverka när det gäller den personliga integriteten.

Det talas ibland också om att elever ges ”digitala tatueringar”, som följer dem under hela deras vandring genom utbildningssystemet och kanske även hänger med ut i arbetslivet. Eleverna ges ingen möjlighet att börja om när de byter skola och kanske inte ens när de slutar skolan.[28] Tatueringarna består i personuppgifter och de analyser som gjorts med hjälp av uppgifterna, och som kanske aldrig gallras. Frågan om digitala tatueringar kan antas växa i betydelse i takt med att inlärningsanalytiska metoder och arbetssätt vinner terräng och börjar användas av skolorna och systemleverantörerna. Problematiken är snarlik den som brukar anföras i samband med sökmotorernas algoritmer, vilket ibland omtalas som nätets ”filterbubblor” eller ”ekokammare”.[29]

Digitala lärplattformar och digitala läromedel

Det är skolornas huvudmän som är personuppgiftsansvariga för hanteringen av personuppgifter i de digitala lärplattformar och digitala läromedel som används vid skolan, men viktiga beslut som handlar om hantering av elevernas personuppgifter kan många gånger i praktiken fattas av enskilda lärare. Huvudmannen har sällan en fullständig överblick över eller insyn i vilka uppgifter som hanteras i systemen, hur de används och hur länge de sparas. Ibland känner huvudmannen över huvud taget inte till vilka system som används i skolan. Det är kommitténs uppfattning att detta är ett allmänt förekommande problem i skolorna i dag.[30]

Därtill kommer att det för elever i grundskolan och gymnasieskolan inte finns någon sekretess eller tystnadsplikt för större delen av den växande uppgiftsmassan.

[28] Se rapporten *Personvern 2015 – tilstand og trender*, från norska Teknologirådet och Datatillsynet, januari 2015.

[29] Se kapitel 12 om konsumentområdet.

[30] Denna iakttagelse görs avseende norska förhållanden, som i detta avseende bör vara mycket lika de svenska, se rapporten *Personvern 2015 – tilstand og trender*, från norska Teknologirådet och Datatillsynet, januari 2015.

En stor andel av undervisningen för landets elever hanteras i digitala lärplattformar och i digitala läromedel. Det rör sig om allt fler och detaljerade uppgifter om varje enskild elev. Dessa uppgifter är av stort intresse för både skolhuvudmän och leverantörer för att dessa ska kunna lära sig mer om eleven, om inlärningsprocesser generellt och om hur plattformar och läromedel fungerar och kan förbättras. Uppgifterna kan därför komma att användas för helt nya ändamål, som eleven och ibland inte heller skolan, känner till och kan påverka. Elevuppgifternas värde innebär också att de kan komma att spridas till exempelvis leverantörernas samarbetsparter. Sekretesskyddet är relativt svagt och det saknas särskild lagstiftning för hanteringen av elevuppgifter, här gäller endast personuppgiftslagen. Sammantaget anser kommittén att användningen av digitala lärplattformar och läromedel innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att digitala lärplattformar och läromedel kan förbättra undervisningen avsevärt och hjälpa eleverna att uppnå sina mål.

Sociala medier i undervisningen

Fyra av tio lärare i gymnasieskolan använder sociala medier för att kommunicera med elever. I kommitténs kontakter med skolföreträdare, har uppgetts att det blir allt vanligare att sociala medier används i undervisningen i svenska skolor.

Användningen av sociala medier kan medföra att ett stort antal närgångna uppgifter om den enskilde oavsiktligen exponeras för andra. Vidare förekommer det att sociala medier använder uppgifterna för egna ändamål och sprider dem vidare till andra företag. Det är också svårt för användarna att få klarhet i hur uppgifterna faktiskt hanteras när användarvillkoren väl har godkänts. Den enskildes valmöjlighet är oftast begränsad till att antingen godkänna samtliga villkor, eller att avböja och därmed helt ställa sig utanför det sociala mediet. I kapitel 13 om sociala medier, bedömer kommittén därför att användningen av vissa sociala medier innebär en allvarlig risk för den personliga integriteten. Risken blir inte mindre vid användning i skolan. Vid sådan användning tillkommer som riskfaktorer att eleverna inte själva får bestämma över det. De blir i stället uppmanade av skolan att använda sociala medier. Skolan bestämmer också hur

eleven ska använda sig av det. Det kan bl.a. leda till en oönskad sammanblandning av uppgifter från elevens privata respektive skolrelaterade verksamheter i det sociala mediet.

Samtidigt måste också beaktas att användningen av sociala medier i skolan kan bidra till undervisningen på ett mycket positivt sätt, bl.a. genom att göra det enklare att omvärldsbevaka, kommunicera och dela material med andra elever, lärare och föräldrar.

Elevhälsan

Inom elevhälsan hanteras känsliga uppgifter om alla elever i skolan. Uppgifterna har ett relativt starkt sekretesskydd och elevhälsans hantering av uppgifter omfattas av patientdatalagen. Det saknas undersökningar ur ett integritetsskyddsperspektiv från senare år om hur personuppgifter från eller inom elevhälsan hanteras i skolorna. Kommittén anser att hanteringen av uppgifter i elevhälsan innebär en viss risk för den personliga integriteten.

Samtidigt måste också beaktas att det är av vikt för elevhälsan, och därmed även för eleverna, att verksamheten kan dra nytta av de fördelar som t.ex. dokumentation i digitala system kan medföra.

Skolfederationen

Skolfederationen är en tjänst som, använd på rätt sätt, kan innebära att uppgifter ges ett bättre skydd och exponeras för leverantörer i mindre omfattning än vad som annars hade varit fallet. Emellertid är skyddet beroende på skolhuvudmännens och leverantörernas kunskaper och val av inställningar i tjänsten, samt deras medvetenhet om personuppgiftsansvarets placering och innebörd. Mot bakgrund av de bristande kunskaperna om integritetsskydd hos många skolhuvudmän, anser kommittén att Skolfederationen innebär en viss risk för den personliga integriteten.

Kameraövervakning i skolor

Kameraövervakning inomhus förekommer sannolikt i ett betydande antal skolor i dag. Det finns skolor som har ett stort antal kameror inomhus. Det kan därför vara svårt för elever att hitta områden som inte övervakas. Men, det får antas att en så omfattande kameraövervakning inte är vanligt förekommande i landets skolor.

Besluten att införa kameraövervakning delegeras inte sällan långt ner i organisationen och dokumentationen av anledningen till övervakningen är ofta bristfällig. De som övervakas i skolorna tillfrågas sällan om kameraövervakningen och om var och för vilka syften det ska få förekomma. Härtill kommer att teknikutvecklingen har gjort det möjligt att hantera bilderna i exempelvis ansiktsigenkänningsprogram. Kameraövervakning är särskilt reglerad i kameraövervakningslagen. Där regleras bl.a. hur information ska lämnas och hur länge bilderna får lagras. Sammantaget anser kommittén att kameraövervakning inomhus i skolor utgör en påtaglig risk för den personliga integriteten.

Samtidigt måste också beaktas att kameraövervakning inomhus i skolor kan vara ett betydelsefullt verktyg för att uppnå säkerhet och trygghet för eleverna. Det saknas dock svenska undersökningar om detta.

8 Arbetslivet

Kommitténs bedömning: Inom arbetslivsområdet finns det såväl företeelser som innebär vissa risker för den personliga integriteten, som företeelser som är förknippade med allvarliga risker. Läs mer om vår bedömning av de olika företeelserna inom området i avsnitt 8.10.

8.1 Inledning

8.1.1 Beskrivning av området

Det här kapitlet handlar om personlig integritet för arbetstagare i vid mening, som t.ex. anställda, arbetssökande, de som söker eller fullgör praktik eller som utför arbete som inhyrd eller inlånad arbetskraft.[1]

Integritetsskyddet i arbetslivet har varit föremål för tre olika utredningar sedan år 2002, som samtliga har konstaterat brister i integritetsskyddet för arbetstagare och föreslagit ändringar och förtydliganden i regelverket. Hittills har emellertid inget av förslagen lett till lagstiftning.[2]

Karaktäristiskt för övervakning inom arbetslivet är att endast få system marknadsförs med det uttalade syftet att övervaka arbetstagarna. Vanligen är det angivna syftet ett annat, men tekniken gör det även möjligt att i detalj övervaka personalen. Ett bra sådant exempel är lösningar för elektronisk körjournal. Dessa bygger på att en GPS hela tiden positionsbestämmer arbetsgivarens bilar. Informa-

[1] Jfr Utredningens om registerutdrag i arbetslivet betänkande *Registerutdrag i arbetslivet*, SOU 2014:48.

[2] Integritetsutredningens betänkande *Personlig integritet i arbetslivet*, SOU 2002:18, Utredningens om integritetsskydd i arbetslivet betänkande *Integritetsskydd i arbetslivet*, SOU 2009:44.

tionen kan arbetstagaren använda för att redovisa till Skatteverket att bilen inte används för privat bruk. Men samtidigt gör tekniken det möjligt för arbetsgivaren att i realtid se var arbetstagaren som framför fordonet befinner sig.

8.1.2 Regelverk och tillsyn

Hanteringen av personuppgifter om arbetstagare regleras i huvudsak av personuppgiftslagen (1998:204), med Datainspektionen som tillsynsmyndighet.[3] Men även arbetsmarknadens parter spelar en viktig roll inom området. De kan exempelvis förhandla om kontrollåtgärder som har inverkan på arbetstagarnas personliga integritet, enligt lagen (1976:580) om medbestämmande i arbetslivet eller ingå kollektivavtal i frågor om personlig integritet.

Den bestämmelse i personuppgiftslagen som oftast aktualiseras inom arbetslivet är 10 § punkten f. Bestämmelsen gör det möjligt för en arbetsgivare att behandla personuppgifter om det är nödvändigt och intresset av att behandla uppgifterna är större än arbetstagarens intresse av att uppgifterna inte behandlas. Bedömningen ska avgöras efter en avvägning. Hur den utfaller beror bland annat på förhållandena på den aktuella arbetsplatsen, vilken slags verksamhet som bedrivs, för vilket ändamål behandlingen ska utföras, vilka regler och riktlinjer som utfärdats av arbetsgivaren och vilken information arbetstagarna har fått.[4]

All behandling av personuppgifter måste vara laglig och ska dessutom utföras på ett korrekt sätt och i enlighet med god sed på arbetsmarknaden. Vad som är god sed kan avgöras mot bakgrund av bland annat överenskommelser inom arbetsmarknaden.

Det kan ofta vara svårt för arbetsgivare att stödja en behandling av personuppgifter på samtycken från arbetstagarna. Det beror på att arbetstagare ofta befinner sig i en beroendeställning gentemot sina arbetsgivare och därför inte kan lämna sådana frivilliga samtycken som personuppgiftslagen kräver. Behandling av personuppgifter i arbetslivet med stöd av samtycke begränsas därför till sådana situationer där arbetstagaren har ett verkligt fritt val och senare kan ta

[3] Även annan lagstiftning kan bli aktuell, såsom exempelvis brottsbalkens bestämmelser om dataintrång. En utförlig redogörelse för regler som kan bli tillämpliga ges i SOU 2009:44, s. 69 f.
[4] Se Datainspektionens informationsbroschyr *Personuppgifter i arbetslivet*, version maj 2014.

tillbaka sitt samtycke utan att det medför några nackdelar. Om de anställda erbjuds rimliga alternativ och inte utsätts för någon direkt eller indirekt påtryckning att samtycka kan det vara tillåtet för arbetsgivaren att behandla personuppgifter med stöd av samtycken från de anställda.[5]

Personuppgiftslagen ställer stora krav på att arbetsgivaren självmant informerar de anställda om vilka personuppgifter som samlas in och vad de ska användas till.[6]

Även lagen om medbestämmande i arbetslivet har betydelse i sammanhanget. Det framgår av lagens 11 § att en arbetsgivare, innan den beslutar om viktigare förändring av sin verksamhet, på eget initiativ ska förhandla med arbetstagarorganisation i förhållande till vilken arbetsgivaren är bunden av kollektivavtal. En sådan viktig förändring kan vara införandet av system, arbetssätt eller andra åtgärder som medför möjligheter till övervakning.

Det förekommer också att kollektivavtal närmare reglerar vilken övervakning av arbetstagarna som får förekomma. Om arbetsgivaren avviker från kollektivavtalet kan en facklig organisation som har kollektivavtal med arbetsgivaren begära allmänt skadestånd för kollektivavtalsbrott.

Rätten att leda och fördela arbetet, den s.k. arbetsledningsrätten, är en allmän rättsgrundsats som innebär att arbetsgivaren inom ramen för anställningsavtalet t.ex. bestämmer om arbetets utförande, platsen för arbetet och arbetsmetoder. Arbetsledningsrätten innebär också att arbetsgivaren bestämmer om vilken teknisk utrustning som ska finnas och hur den ska användas. Arbetsledningsrätten kan också innefatta en rätt att vidta kontrollåtgärder, t.ex. genom kameraövervakning. Arbetsledningsrätten får dock inte utövas i strid mot lag eller god sed på arbetsmarknaden.

För myndigheter finns även särskilda bestämmelser i offentlighets- och sekretesslagen (2009:400) som rör arbetslivet samt bestämmelser om bevarande och gallring i tryckfrihetsförordningen och arkivlagen (1990:782). Även bestämmelsen i regeringsformens 2 kap. 6 § kan bli aktuell när arbetsgivaren är en myndighet.[7] Enligt bestämmelsen är var och en är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp, kroppsvisitation, husrannsakan och

[5] Se Datainspektionens informationsbroschyr *Personuppgifter i arbetslivet*, version maj 2014.
[6] *Personuppgifter i arbetslivet.*
[7] Se t.ex. AD 1984 nr 94.

liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Enligt bestämmelsen är också var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Om en enskild arbetstagare anser att hans eller hennes personuppgifter hanterats på ett felaktigt sätt och vill vända sig till en statlig myndighet med sitt klagomål, bör han eller hon i första hand vända sig till Datainspektionen.

Därtill utövar Riksdagens ombudsmän (Justitieombudsmannen) och i viss mån Justitiekanslern tillsyn över det allmännas verksamhet. Polis och åklagare kan utreda misstänkta brott.

Vid behandling av en arbetstagares personuppgifter i strid mot personuppgiftslagen blir skadeståndsbestämmelsen i 48 § personuppgiftslagen tillämplig. Enligt den bestämmelsen är den personuppgiftsansvarige skyldig att ersätta den registrerade för skada och kränkning av den personliga integriteten som orsakats av en behandling i strid med lagen.

Vidare kan det finnas en viss möjlighet för en arbetstagare att begära skadestånd för den skada som hon eller han anser sig ha lidit på grund av integritetsintrång enligt 2 kap. 3 § skadeståndslagen (se vidare kapitel 23 om vilket skydd samhället erbjuder).[8]

Den praxis som finns från Arbetsdomstolen rörande tillämpning av personuppgiftslagen handlar om alkoholkontroller[9], bärande av namnskylt[10] samt om arbetsgivares utlämnande av löneuppgifter och anställningsbevis till fackliga organisationer.[11]

Det finns också möjlighet för en arbetstagare att få allmänt och ekonomiskt skadestånd om denne blivit föremål för disciplinära åtgärder, t.ex. vid en uppsägning som grundar sig på att en arbetstagare vägrat att underkasta sig kontrollåtgärder om dessa utförts i strid mot gällande rätt.[12]

---

[8] Utredningen om personlig integritet i arbetslivet uttryckte emellertid tveksamhet till att bestämmelsen i skadeståndslagen kunde medföra rätt till skadestånd avseende brott mot den personliga integriteten i arbetslivet, se SOU 2012:18.

[9] AD 2009 nr 63 och AD 2013 nr 19.

[10] AD 2013 nr 29.

[11] AD 2009 nr 3 och AD 2010 nr 87.

[12] Se regler om skadestånd i LAS 38–39 §§.

Europakonventionens artikel 8 om rätt till respekt för en enskilds privat- och familjeliv, hem och korrespondens ger ett skydd mot olika former av intrång i den enskildes sfär och är tillämplig på förhållanden i arbetslivet.[13] I Arbetsdomstolens praxis finns avgöranden som direkt grundar sig på Europakonventionen och som berör såväl privata som offentliga arbetsgivare.[14] Rätten till skydd för den personliga integriteten får inskränkas genom lag om det i ett demokratiskt samhälle är nödvändigt med hänsyn till de syften som anges i artikel 8.2. Enligt konventionen får rätten till skydd för den personliga integriteten inskränkas, om inskränkningen står i rimlig proportion till det syfte som ska uppnå med den. Varje konventionsstat ges ett visst handlingsutrymme att besluta om en inskränkning är nödvändig. Omfattningen av handlingsutrymmet varierar beroende på frågans natur och de berörda intressenas vikt. Ett sådant intresse kan till exempel vara arbetsgivarens arbetsledningsrätt som innefattar en rätt att vidta kontrollåtgärder. I målet Wretlund mot Sverige som berörde en arbetstagares skyldighet att underkasta sig drogtestning fann Europadomstolen att drogtestningen kunde rättfärdigas med stöd av artikel 8.2.[15]

Vidare finns det en rekommendation från Europarådet om integritetsskydd i arbetslivet, antagen den 1 april 2015 av ministerkommittén, som innehåller detaljerade rekommendationer för behandlingen av personuppgifter i arbetslivet.[16] Rekommendationen tar sin utgångspunkt i globaliseringen och den ökade användningen av IKT (informations- och kommunikationsteknik) på arbetslivets område. Rekommendationen berör bl.a. när och hur arbetsgivare får hantera uppgifter om arbetstagares hälsa och genetiska data, uppgifter om arbetstagares användning av internet samt uppgifter om arbetstagares privata användning av arbetsplatsens mejlsystem. I rekommendationen uttalas att det inte bör vara tillåtet för arbetsgivare att använda sig av system vars främsta syfte är att övervaka arbetstagarnas aktiviteter och beteenden. Nya ändamål för han-

[13] Se t.ex. SOU 2009:44 s. 195 ff.

[14] Se t.ex. AD 1998 nr 17 och AD 2011 nr 15.

[15] Se Application no. 46210/99.

[16] *Recommendation CM/Rec (2015) 5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*. Rekommendationen är en revidering av den tidigare *Recommendation Rec (89) 2 of the Committee of Ministers to member States on the protection of personal data for employment purposes*. Den nya rekommendationen ersätter den äldre rekommendationen.

teringen av arbetstagarnas uppgifter, bör enligt rekommendationen inte förekomma annat än under särskilda omständigheter. I rekommendationen behandlas flera av de frågor som tas upp i författningsförslaget som lämnades i betänkandet *Integritetsskydd i arbetslivet*.[17]

8.2 Positionering

8.2.1 Företeelsen

Många system som används i arbetslivet i dag innehåller funktioner för att kunna positionera utrustningen och därmed den arbetstagare som använder utrustningen.

Positioneringstekniken kan ha många fördelar för både arbetsgivare och arbetstagare. Positionering gör det möjligt att på ett enkelt sätt redovisa till olika myndigheter hur t.ex. fordon används. Den gör det också möjligt att styra arbetstagare och fordon till rätt platser i realtid, spåra borttappad eller stulen utrustning och att snabbt kunna hitta och hjälpa arbetstagare som hamnar i hotfulla situationer m.m.

8.2.2 Elektroniska körjournaler

Det finns skatterättsliga bestämmelser som kräver att arbetstagare som har dispositionsrätten till en bil måste kunna visa att bilen används endast i ringa omfattning för privat körning. Ett sätt att visa detta är att dokumentera samtliga resor (både i tjänsten och privata) i en körjournal, som enklast förs elektroniskt.

I system för elektronisk körjournal installeras en GPS-enhet (inte mycket större än en tändsticksask) i bilen som löpande registrerar bilens position. Uppgifter om körningarna kan sparas i åtskilliga år hos systemleverantörerna.

Vissa lösningar använder mobiltelefonteknik för att hela tiden rapportera bilarnas position till en central server. Andra lösningar registrerar bara körningarna i ett internt minne, som arbetsgivaren sedan måste ansluta till en persondator för att kunna tömma på data. Med den sistnämnda lösningen går det inte att övervaka bilens position i realtid.

[17] SOU 2009:44.

Det finns lösningar som har stöd för att hantera bilar som har olika förare. Föraren loggar då in med sitt digitala ID-kort eller passerbricka för att identifiera sig. Kortet innehåller ett chip som kan registreras av en läsare i bilen. När föraren håller kortet framför avläsaren, skickas en signal till den centrala databasen, som verifierar att föraren är inloggad.

Datainspektionen har granskat användningen av ett system för elektroniska körjournaler. I granskningen kom Datainspektionen fram till att företaget som använde GPS-positionering av fordon för elektroniska körjournaler fick göra det utan att först få förarnas godkännande. Det förutsatte dock att ett antal villkor måste vara uppfyllda, bland annat fick inte fler uppgifter än nödvändigt samlas in av systemet.[18]

8.2.3 Fordonskontroll

Fordonskontroll, eller *fleet management* som det också kallas, bygger på samma princip som elektronisk körjournal. Syftet med fordonskontroll är dock ett annat. Här handlar det om att kunna dirigera bilar effektivt, så att man skickar det fordon som är närmast en aktuell kund.

Även i system för fordonskontroll monteras en GPS-enhet i alla fordon som arbetsgivaren vill bevaka. Arbetsgivaren kan sedan i realtid se positionen för varje fordon.

8.2.4 Digitala färdskrivare

Det finns regler som kräver att nytillverkade bussar och tunga lastbilar är utrustade med digitala färdskrivare.[19] I färdskrivarna registreras uppgifter om förarens kör- och vilotider. I flera system överförs sedan uppgifterna trådlöst till en central dator hos arbetsgivaren.

[18] Datainspektionens beslut den 7 februari 2014 i dnr 234-2013.
[19] Rådets förordning (EEG) nr 3821/85 av den 20 december 1985 om färdskrivare vid vägtransporter.

8.2.5 Körstil

Det finns särskilda system som övervakar hur fordonen framförs, om föraren kör på ett ekonomiskt och miljövänligt sätt, eller om föraren är aktiv på de tidpunkter och på det sätt som arbetsgivaren önskar. Samma system som används för att uppfylla kraven i olika regelverk kan också innehålla tilläggsfunktioner som kan användas för att kontrollera hur fordonet framförs.

Systemen fungerar vanligtvis genom att fordonet i fråga förses med en sändare som skickar uppgifter om fordonet till systemleverantören. Det kan röra sig om uppgifter om fordonets position, dess rörelser (såsom acceleration, svängar och inbromsningar som registreras av en gyroskopisk sensor), bränsleförbrukning, hastighet och förarens identitet m.m.

Arbetsgivaren kan få åtkomst till uppgifterna både i realtid och i form av sammanställningar. Inte sällan ges åtkomst till uppgifterna genom en mobilapp, vilket innebär att uppgifterna kan komma att spridas till ännu fler aktörer, exempelvis till appens eller mobiltelefonens tillverkare.

Utöver sådana särskilda system som arbetsgivaren skaffar, kan fordonen redan när de levereras från fabrik vara försedda med system som samlar in uppgifter om fordonet och trådlöst skickar dem vidare till fordonstillverkaren.

Vissa fordon är inte i förväg byggda för att trådlöst kommunicera uppgifter, utan lagrar endast dessa internt. Dessa uppgifter kan sedan laddas ner exempelvis till ett usb-minne av arbetsgivaren eller när fordonet är inne på verkstad för att genomgå service.

Ett system som hanterar uppgifter om körstil behandlades i ett ärende hos Datainspektionen.[20] I ärendet ville ett bolag använda sig av en tjänst kallad ”Trafiksäkerhet” som tillhandahölls av en extern leverantör. Tjänsten byggde på s.k. *ISA-teknik* (intelligent stöd för anpassning av hastighet). Information från nationella vägdatabasen kombinerades med fordonets position för att visa aktuell lagstadgad hastighet på den vägsträcka som fordonet framfördes på samt den aktuella hastighet som fordonet hade.

ISA-tekniken bestod av tre komponenter: en GPS-mottagare, en minidator och en supportenhet med en skärm som visade gällande hastighetsbegränsning och en varningssignal som började låta om

[20] Datainspektionens beslut den 18 november 2013 i dnr 768-2013.

hastighetsbegränsningen överträddes. Tekniken innebar att föraren i realtid på sin fordonsskärm kunde se hur stor del av körtiden som han eller hon hade hållit sig till lagstadgad hastighet respektive kört för fort. Bolagets syfte med tjänsten ”Trafiksäkerhet” var att minska riskerna i trafiken genom att föraren skulle framföra fordonet i enlighet med gällande hastighetsbegränsning. Den lägre hastigheten skulle uppnås genom att föraren fick direktåterkoppling via fordonsskärmen. Även sammanställda förarrapporter syftade till att göra föraren uppmärksam på hur han eller hon hade framfört fordon i tjänsten under den gångna arbetsperioden och om det fanns skäl att fundera över sin körstil (hastighet). Eftersom det rörde sig om uppgifter om hastighetsöverträdelser, ansåg Datainspektionen att det var frågan om uppgifter om lagöverträdelser i personuppgiftslagens mening. Därmed krävdes ett beslut om undantag från det principiella förbudet i 21 § personuppgiftslagen från Datainspektionen för att bolagets hantering skulle vara laglig. Vid en samlad bedömning kom Datainspektionen fram till att bolaget skulle få använda sig av den aktuella tjänsten, om bolaget uppfyllde en rad olika krav rörande bl.a. information till förarna, begränsning av hur bolaget använde sig av uppgifterna och ett tillräckligt bra skydd för uppgifterna.

8.2.6 Positionering i annan utrustning

Teknik för positionering kan även finnas i annan utrustning än fordon, såsom i smarta enheter som surfplattor och mobiler eller andra typer av handhållna enheter.

Ett aktuellt exempel är GPS-enheter i surfplattor. Ett mål i Arbetsdomstolen gällde servicemontörer vid ett bolag som upptäckte att GPS-enheter hade installerats och aktiverats i de surfplattor som arbetsgivaren försett dem med och som användes i tjänsten. GPS-funktionen gick inte att stänga av utan angivande av ett lösenord, vilket bolaget ensamt hade tillgång till. Enligt stämningsansökan hade servicemontörerna inte informerats i förväg om bolagets åtgärd och inte heller lämnat samtycke till behandling av deras personuppgifter. Bolaget hade före införandet av GPS-positioneringen enligt stämningsansökan inte heller fullgjort sin skyldighet att genomföra förhandlingar med Svenska Elektrikerförbundet i enlighet med det mellan parterna gällande kollektivavtalet. Svenska Elektrikerförbundet hade i

målet yrkat att bolaget skulle förpliktas att utge allmänt skadestånd till förbundet och till var och en av de berörda servicemontörerna enligt personuppgiftslagen.[21]

Inom hemtjänsten används positioneringsteknik för att kontrollera insatser som utförs hemma hos brukare. Det finns olika tekniska lösningar för sådan rapportering. Vissa bygger på att personalen vid hemtjänsten använder en smart telefon eller surfplatta, medan andra bygger på en speciell digital penna och etiketter. Principen är dock genomgående att personalen registrerar när man kommit på hembesök, vad man gjort under besöket och när man gick. Via mobiltelefonens GPS bekräftas att personalen verkligen varit på plats. Med en digital penna görs samma sak genom att läsa av en etikett som sitter på dörrkarmen hos den person där man gör hembesök, liknande det förfarande som används av övervakningsföretag. Med vissa av dessa tekniker kan arbetsgivaren i realtid följa arbetstagarnas rörelser ner på meter- och minutnivå.

Inom socialtjänsten i Stockholm har användningen av positioneringen och kontrollen av arbetstagarna lett till diskussioner och det s.k. Hemtjänstupproret på Facebook.[22]

Enligt uppgifter i media bedömer Sveriges Kommuner och Landsting att hemtjänsten i minst 50 kommuner har elektronisk rapportering.[23]

Vidare använder allt fler företag någon form av verktyg för att hantera arbetstagarnas tjänstemobiler. Sådana lösningar förkortas MDM, vilket står för *Mobile Device Management*. De fungerar genom att en speciell app installeras på mobilen. Via appen kan en administratör bland annat fjärradera mobiltelefonen om den skulle tappas bort eller bli stulen. Men vanligen går det att göra betydligt mer än så med hjälp av appen. Exempelvis kan administratören se vilka andra appar som är installerade, förhindra att vissa appar installeras och bestämma hur lång pinkod eller lösenord som måste användas för att låsa upp telefonen. Ofta går det också att positionera telefonen vilket innebär att administratören på en karta kan se var telefonen befinner sig i realtid.

[21] Arbetsdomstolens mål nr A 92/13. Målet avgjordes inte genom dom, utan talan återkallades och målet avskrevs.

[22] Malin Beeck, *Storebror ser dig – om du jobbar i hemtjänsten*, publicerad den 7 februari 2014 på www.etc.se

[23] Anna Lena Wallström, *Uppror mot kontroll i hemtjänsten*, publicerad den 11 augusti 2014 på www.dn.se

Vissa MDM-verktyg stöder dessutom s.k. *geo-fencing*, vilket innebär att administratören får ett larm om telefonen bärs utanför ett visst geografiskt område som administratören har bestämt. När larmet går ut kan t.ex. mobiltelefonens minne automatiskt raderas.

8.2.7 Risker för den personliga integriteten

Positioneringsteknik blir allt enklare och billigare. Det betyder att det finns en risk för att positionering av arbetstagare kommer att börja användas i ännu större utsträckning än i dag, helt enkelt för att det är möjligt. I vissa fall känner varken arbetsgivare eller arbetstagare till att utrustningen faktiskt positionerar användaren, eftersom dessa uppgifter lagras hos utrustningens tillverkare eller hos en mjukvaruleverantör.

Det finns även en risk för att fler uppgifter än nödvändigt hanteras om arbetstagarna, och att dessa uppgifter får en spridning som inte arbetstagarna och kanske inte ens arbetsgivarna är fullt medvetna om. Det är därmed också svårt för arbetstagarna att kunna veta för vilka ändamål uppgifterna hanteras.

När detaljerade uppgifter om arbetstagarnas rörelser blir åtkomliga för arbetsgivaren i realtid, finns det också en risk för att uppgifterna kommer att börja användas för helt andra ändamål än vad som ursprungligen var avsikten. Risken för detta förefaller vara särskilt stor när det gäller arbetstagare som utför ensamarbete, såsom chaufförer och hemtjänstpersonal. I media har rapporterats om flera fall då positioneringsutrustning i fordon som ursprungligen installerats för att exempelvis underlätta logistik, öka chaufförernas säkerhet eller främja miljön, även kommit att användas för att på detaljnivå kontrollera och ifrågasätta alla chaufförernas aktiviteter som pauser, kortare tids stillastående och val av färdväg m.m.[24]

Uppgifter om en arbetstagares position kan också sammanställas med andra uppgifter om arbetstagaren och användas för nya ändamål, exempelvis riktade annonser.

[24] Johanna Kvarnsell, *Gps ger chefen koll i realtid*, publicerad i tidningen Transportarbetaren den 31 januari 2014.

Det finns också en risk att uppgifter om arbetstagarens position kan läcka ut på grund av brister i skyddet och användas i syfte att förbereda brott, exempelvis inbrott när arbetstagaren är bortrest i tjänsten, för att förfölja en person eller genom att användas som bakgrundsinformation inför identitetsstöld och bedrägeribrott.

Ofta lagras positioneringsuppgifterna i en molntjänst och kan då komma att hanteras av underleverantörer till systemleverantören. Det innebär en risk för att uppgifterna sprids utanför arbetsgivarens kontroll till tredje land.

8.3 Övervakning av aktiviteter och beteenden

8.3.1 Företeelsen

De system som omnämns i delavsnittet ovan, möjliggör förutom positionering även att en rad andra uppgifter om arbetstagaren registreras och hanteras.

Många system som är i bruk på arbetsplatserna i dag, genererar en stor mängd uppgifter om användarna. Ofta behövs uppgifterna för att exempelvis kunna styra behörigheter och i efterhand kunna göra felsökningar eller kontrollera åtkomsten till integritetskänsliga uppgifter om arbetsgivarens kunder.

I dag vistas många arbetstagare på arbetsplatser där det förekommer kontroll eller övervakning av verksamhetens kunder, patienter eller brukare. Men eftersom arbetstagarna befinner sig i samma lokaler, kommer även de att träffas av arbetsgivarens övervakning. Det kan exempelvis röra sig om butiker som använder sig av s.k. *WiFi-Tracking* i syfte att få veta hur kunderna rör sig inne i butiken. I dessa fall kommer även arbetstagarnas mobiltelefoner att inbegripas i kartläggningen av rörelsemönster. Detsamma kan även göras inom exempelvis äldreomsorgen i takt med att det blir vanligare att äldreboenden förses med utrustning såsom rörelsedetektorer eller trycksensorer i golven m.m.

8.3.2 Internet och e-post

Det finns en rad olika verktyg på marknaden för övervakning av hur arbetstagare använder arbetsgivarens utrustning, t.ex. för att surfa på nätet eller skicka och läsa e-post.

Ett exempel som kan nämnas är tjänsten *ActivTrak*. Den bygger på att ett litet program installeras på varje arbetstagares dator. Programmet installeras dolt och visas aldrig för användaren, men rapporterar hela tiden vad användaren gör till en molntjänst. Där kan arbetsgivaren i ett gränssnitt se en rad uppgifter, som vilka program som körs, vilka webbsidor som besöks m.m. Det går att klassa webbplatser som ”produktiva” och ”icke-produktiva”. Det går även att få ut statistik över hur mycket en arbetstagare ägnar åt att besöka ”icke-produktiva” sajter.

Vissa av dessa verktyg är till och med kostnadsfria för arbetsgivaren om bara ett mindre antal personer ska övervakas.

Det finns också särskilda program som gör det möjligt för en arbetsgivare att upptäcka och förhindra att arbetstagare obehörigen röjer känslig information till utomstående, s.k. *Data Loss Prevention Tools* (DLP-verktyg). Dessa program gör det exempelvis tydligt för arbetsgivaren var känslig information lagras och vilka som hanterar den. Programmen kan också skicka en varning till arbetsgivaren om känslig information används på något ovanligt eller avvikande sätt. I de fall arbetsgivaren tillåter eller rentav uppmanar arbetstagarna att använda sin egen, privata IKT-utrustning i tjänsten (s.k. BYOD-lösningar, från *Bring Your Own Device*), kommer även arbetstagarens hantering av rent privat information att övervakas och kontrolleras genom DLP-verktyget. Datainspektionen har i ett ärende uttalat att den inte ser några principiella hinder enligt personuppgiftslagen mot att en arbetsgivare använder DLP-verktyg, under förutsättning att arbetsgivaren följer alla relevanta bestämmelser i personuppgiftslagen.[25]

Det finns ingen statistik eller andra uppgifter om hur pass utbredd användningen av sådana här verktyg är i Sverige. År 2007 genomförde American Management Association en undersökning om arbetsplatser i USA.[26] Undersökningen visade att 66 procent av de till-

[25] Datainspektionens beslut den 8 oktober 2013 i dnr 1250-2013.

[26] Se rapporten *2007 Electronic Monitoring & Surveillance Survey* från American Management Association.

frågade arbetsgivarna övervakade internettrafiken och att 65 procent använde verktyg för att blockera ”olämpliga” webbplatser. 43 procent av de tillfrågade arbetsgivarna övervakade mejltrafiken.

Det blir allt vanligare att arbetsgivare tillåter, och ibland till och med uppmuntrar, arbetstagarna att använda sig av arbetsgivarens utrustning såsom datorer och smarta telefoner även för rent privat kommunikation. Det finns även ekonomisk stimulans från statligt håll för sådant bruk, genom att viss privat användning av utrustning är tillåten utan att det utlöser förmånsbeskattning för arbetstagaren.[27]

8.3.3 Personliga konton

Många arbetsgivare tillhandahåller utrustning till arbetstagarna i form av datorer och smarta enheter som mobiltelefoner eller surfplattor. Utrustningen innehåller programvaror som behövs för att utföra arbetet, exempelvis operativsystem, program för ordbehandling och för e-post.

Användningen av dessa program kräver emellertid ofta att arbetstagaren registrerar sig som användare hos systemleverantören. Till exempel kräver vissa versioner av Microsofts operativsystem Windows att varje användare (i detta sammanhang varje arbetstagare) skaffar sig ett personligt Microsoft-konto. Androidtelefoner kan kräva att varje användare skaffar sig ett personligt Google-konto. Den senaste versionen av Windows har blivit kritiserad för att den möjliggör för Microsoft att samla in stora mängder uppgifter om enskilda användare.[28]

Systemen i den utrustning som arbetsgivarna tillhandahåller, är allt oftare molnbaserade.

En annan situation när arbetstagare kan behöva använda sig av ett personligt konto i tjänsten, är då han eller hon som en del i arbetet använder sig av e-tjänster som kräver inloggning med e-legitimation, exempelvis för att elektroniskt lämna arbetsgivarens moms- och arbetsgivardeklarationer till Skatteverket. Det finns i dagsläget ingen e-legitimation för juridiska personer, utan arbetstagaren måste använda sig av sin personliga e-legitimation för att för arbetsgivarens räkning kunna nyttja myndigheternas e-tjänster.

---

[27] Se exempelvis Skatteverkets ställningstagande *Förmånsbeskattning av elektronisk utrustning eller abonnemang mot fast avgift* (Skatteverkets dnr 131 555207-13/111).

[28] Olle Nygårds, *Nya Windows sågas för massiv datainsamling*, publicerad den 6 augusti 2015 på www.svd.se

8.3.4 Ärendehanteringssystem

Vidare används på många arbetsplatser olika slags ärendehanteringssystem, som ofta har funktioner för att kunna visa vilken arbetstagare som varit aktiv i systemet och vad han eller hon har gjort.[29] Ofta sparas information om alla händelser i systemet i syfte att åstadkomma så stor spårbarhet som möjligt.

I ett ärende hos Datainspektionen användes uppgifter om när en viss arbetstagare loggade in på arbetsplatsens olika it-verktyg, för att kontrollera om arbetstagaren redovisade rätt antal timmar.[30] Kontrollen gjordes efter att misstanke om brott mot anställningsavtalet uppkommit. Datainspektionen kom fram till att arbetsgivarens intresse av att kontrollera sina anställda i detta fall vägde tyngre än den anställdes intresse av integritetsskydd. Enligt beslutet måste arbetsgivaren informera alla arbetstagare om vilka kontroller som kan komma att göras och vad syftet med kontrollerna är.

I ett annat ärende granskade Datainspektionen hur uppgifter om arbetstagare vid ett callcenter hanterades.[31] Från ärendesystemet sammanställdes veckovis uppgifter om antalet påbörjade och avslutade ärenden som respektive handläggare hade presterat under en vecka. Syftet med detta var att följa upp verksamhetens produktion och inhämta underlag för lönesättning. Vidare lagrades alla uppgifter om telefonin. En gång i månaden gjordes en sammanställning på handläggarnivå, i syfte att kontrollera åtkomst och tillgänglighet i arbetsgivarens tjänster och se till att bemanningen i callcentret var tillräcklig. Datainspektionen ansåg att det är lämpligt att den här typen av frågor i första hand löses mellan arbetsgivaren och de fackliga organisationerna. Därefter gjorde Datainspektionen emellertid bedömningen att arbetsgivaren i detta fall med stöd av en intresseavvägning enligt 10 § personuppgiftslagen fick behandla personuppgifterna på beskrivet sätt och för de angivna ändamålen. Datainspektionen betonade samtidigt att arbetstagarna måste få tillräcklig information om kontrollerna.

[29] Ibland finns det integritetsskyddande lagstiftning som kräver detta, t.ex. följer det av patientdatalagen att arbetstagares åtkomst till uppgifter om patienter måste följas upp och kontrolleras i efterhand.

[30] Datainspektionens beslut den 22 september 2006 i dnr 1897-2005.

[31] Datainspektionens beslut den 13 maj 2009 i dnr 92-2009.

Vid en granskning år 2002 av 57 olika arbetstagares hantering av uppgifter om individuella arbetstagares prestationer i bl.a. ärendesystem och telefoni, konstaterade Datainspektionen bl.a. att flera arbetsgivare inte hade bestämt varför de hanterade dessa uppgifter om arbetstagarna (dvs. att de inte närmare hade bestämt vilka kontroller man planerade att genomföra med hjälp av uppgifterna) och att de därför inte heller kunde ge arbetstagarna tillräcklig information om hanteringen.[32] Flertalet arbetsgivare hade heller inte klart för sig med vilket lagligt stöd som personuppgifterna hanterades. Den omfattande granskningsinsatsen hade föranletts av att Datainspektionen fått många frågor och en del klagomål från arbetstagare. Många hade handlat om verksamheter i callcenter.

Överhuvudtaget utmärker sig verksamheter i callcenter för att kontrollera arbetstagarna på flera, mycket detaljerade sätt i realtid. Exempelvis är det i branschen vanligt med realtidsövervakning av hur arbetstagarna svarar på samtal, hur länge samtalen varar och om och när de loggar ur sig från telefonsystemen. Vidare är medlyssning och inspelning av telefonsamtal vanligt förekommande, liksom kontroll av e-post och internetanvändning.[33]

8.3.5 In- och utpasseringssystem

På de flesta arbetsplatser förekommer i dag elektroniska in- och utpasseringssystem i vilka någon form av kort används som nycklar och där aktiviteter i systemet registreras på individnivå och därefter lagras.

Ändamålet med att hantera personuppgifter i systemen är oftast att kunna styra vem som ska få tillträde till alla eller vissa av arbetsgivarens olika lokaler samt att kunna göra felsökningar och tekniska kontroller.

Uppgifterna från sådana system kan dock även komma att användas för andra syften. I ett ärende hos Datainspektionen användes uppgifter om en anställd som registrerats i in- och utpasseringssystemet för att kontrollera om den flextiden som arbetstagaren rapporterat avvek från de tider som registrerats i in- och utpasserings-

[32] Datainspektionens rapport 2003:3, *Behandling av personuppgifter om anställda*.
[33] Se Hejlskov, Emma: *Integritet i arbetslivet – en studie om övervakning via telefoner, datorer och positionssystem*, Kandidatuppsats i handelsrätt, HT2013, Lunds universitet, Ekonomihögskolan.

systemet.[34] Det ändamål som arbetsgivaren hade angett med in- och utpasseringssystemet, var att upprätthålla säkerheten för myndighetens lokaler. De anställda hade inte fått någon tydlig information om att deras uppgifter i in- och utpasseringssystemet kunde komma att i undantagsfall användas i samband med kontroll av redovisad arbetstid. Datainspektionen fann ändå att arbetsgivarens kontroll av arbetstid med hjälp av personuppgifterna i sitt in- och utpasseringssystem var tillåten, under förutsättning att det fanns särskild anledning att misstänka att en anställd begår oegentligheter eller missbrukar tidredovisningen. Datainspektionen förutsatte i sitt beslut att arbetsgivaren fortsättningsvis skulle lämna tydligare information till arbetstagarna om arbetsgivarens personuppgiftsbehandling.

8.3.6 Flödes- och logistiksystem

I flera branscher finns det system för att kontrollera flöden och logistik vilka också innebär en övervakning av arbetstagarna.

I varumottagningar och på lager förekommer exempelvis s.k. *Pick-by-Voice*-system. I dessa är det en dator som kontrollerar vilka varor som ska flyttas, och som med röstinstruktioner styr arbetstagaren till rätt plats och vara. I systemet går det att kontrollera och styra hur arbetstagarna arbetar med flödet av varor. Det går också att ta ut tidsloggar ur systemet, som på individnivå visar hur arbetstagare arbetar och tar raster. Datainspektionen har granskat ett sådant system och kunde inte se något principiellt hinder mot att arbetsgivaren – utan arbetstagarnas samtycke – behandlade deras personuppgifter för att tillämpa prestationsbaserad lönesättning och för att få underlag till individuella uppföljningssamtal.[35] Datainspektionen såg inte heller något principiellt hinder mot att bolaget behandlade arbetstagarnas personuppgifter genom realtidsövervakning för att kunna planera och styra arbetet. Däremot ansåg Datainspektionen att det inte var motiverat att använda systemet i syfte att i realtid övervaka hur de anställda utför sina arbetsuppgifter och när de tar raster.

På vissa arbetsplatser tillhandahåller arbetsgivaren särskilda arbetskläder och ser även till att plaggen tvättas. För att kunna kontrollera både det aktuella klädbehovet på arbetsplatsen och tvättprocessen,

[34] Datainspektionens beslut den 14 januari 2013 i dnr 1369-2012.
[35] Datainspektionens beslut den 30 november 2011i dnr 695-2011.

förekommer det att varje plagg förses med en RFID-tagg.[36] På vissa sjukhus finns det klädautomater där arbetstagaren först drar sitt kort och sedan kan hämta ut de kläder som personen i fråga har rätt att ta ut.[37] Systemen kan innehålla funktioner för att visa hur ofta och när arbetstagaren byter kläder.

I delar av restaurangbranschen förekommer kassasystem som registrerar varje maträtt och dryck som beställs samt alla betalningar som görs, och som kopplar alla sådana data till de arbetstagare som medverkat i beställningen. Vissa kassasystem kan även kompletteras med system som hjälper arbetsgivaren att upptäcka svinn och misstänkta stölder och kan koppla detta till individuella arbetstagare. I en studie som genomfördes i restaurangbranschen i USA, framkom att system av det sistnämnda slaget bidrar både till att reducera svinn och till att öka de övervakade arbetstagarnas produktivitet.[38] Det bör dock sägas att det från andra länder och branscher finns forskning som visar på motsatsen, dvs. att arbetstagare som inte övervakas är mer produktiva.[39]

8.3.7 Risker för den personliga integriteten

Det finns en risk för att systemen genererar fler uppgifter på individnivå än som egentligen behövs för verksamhetens bedrivande.

Det finns också en risk för att onödigt många uppgifter hamnar hos systemleverantörer, när t.ex. ett gemensamt Google-konto för flera arbetstagare egentligen är fullt tillräckligt för att upprätthålla funktionaliteten i systemet. I sammanhanget bör emellertid även sägas att gruppinloggningar kan skapa andra problem på grund av den försämrade spårbarhet som sådan inloggning innebär.

När arbetstagare måste registrera personliga konton hos systemleverantörer innebär det att leverantören kan sammanföra uppgifter om arbetstagaren med uppgifter som kommer från arbetstagarens rent privata aktiviteter hos samma leverantör. Det innebär en risk för sammanblandning av privatliv och artbetsliv och en möjlighet för

[36] RFID-taggar berörs närmare i kapitel 12 om konsumentområdet.
[37] Lina Rosengren, *De tvättar kläder med rfid-chip*, publicerad den 27 mars 2013 på www.cio.idg.se
[38] Pierce, Snow & McAfee, *Cleaning house: The Impact of Information Technology Monitoring on Employee Theft and Productivity*, MIT Sloan Research Paper, 24 augusti 2013.
[39] Se t.ex. forskning som återges i Rosenblat, Kneese & Boyd, *Workplace Surveillance*, Data & Society Working Paper, 8 oktober 2014.

systemleverantören att göra en heltäckande kartläggning av arbetstagaren. Det finns troligen en låg medvetenhet om denna risk hos arbetstagarna men också hos arbetsgivarna.

Risken för sammanföring av uppgifter från enskildas privatliv och deras arbetsliv blir större med nya arbetssätt, som när det ges möjlighet att distansarbeta och möjlighet att använda arbetsgivarens utrustning, exempelvis smarta telefoner eller bärbara datorer, för privat bruk.

Många system där det förekommer uppgifter om arbetstagarna är molnbaserade, exempelvis system för mejl- och dokumenthantering, och innebär risker för att uppgifterna sprids till underleverantörer och tredje land och används för nya ändamål, inte sällan utan att arbetstagarna får någon information om det från arbetsgivaren.

8.4 Registerkontroller och medicinska undersökningar

8.4.1 Företeelsen

Inom arbetslivet har det på senare år blivit allt vanligare att arbetsgivare vill att arbetstagare, både arbetssökande och redan anställda, ska uppvisa utdrag ur olika register eller genomgå olika slags medicinska kontroller.

Frågan om arbetsgivares lagliga möjligheter att begära sådana registerutdrag eller medicinska undersökningar, har på senare år ägnats stor uppmärksamhet och varit föremål för två statliga utredningar.

I betänkandet *Integritetsskydd i arbetslivet*[40] föreslogs bl.a. att arbetsgivare, utan stöd i lag eller annan författning, inte ska få begära att en arbetstagare uppvisar ett utdrag ur belastningsregistret, ur misstankeregister eller ur register som förs hos Försäkringskassan (om utdraget innehåller uppgifter för vilka sekretess gäller gentemot arbetsgivaren). Vidare uppställdes i betänkandet förslag på villkor som skulle gälla för arbetsgivares möjlighet att begära att en arbetstagare ska genomgå en medicinsk undersökning eller delge arbetsgivaren resultatet av en medicinsk undersökning. Med medicinsk undersökning avsågs här hälsoundersökningar samt alkohol-, narko-

[40] SOU 2009:44.

tika- eller andra drogtester. Dock omfattades inte alkoholtest som görs med användning av alkolås i fordon. Betänkandet har hittills inte lett till lagstiftning, men bereds i regeringskansliet.

Frågan om uppvisande av utdrag ur belastningsregistret har härefter även utretts av Utredningen om registerutdrag i arbetslivet. I sitt betänkande[41] har utredaren föreslagit att arbetsgivare inte ska få begära att arbetstagare uppvisar eller överlämnar ett utdrag ur belastningsregistret om inte en sådan begäran har stöd i lag eller annan författning.

8.4.2 Risker för den personliga integriteten

De risker för den personliga integriteten som behandlas i 2009 års betänkande rör främst registerkontroller samt medicinska kontroller. Bland annat nämns att det finns en risk att arbetsgivaren får ta del av överskottsinformation som kan finnas både i registerutdrag och i resultaten av medicinska kontroller. När det gäller annan övervakning av arbetstagare förs i betänkandet ett mer principiellt resonemang och konkreta risker och företeelser tas bara upp i korthet.

I 2014 års betänkande nämns exempelvis att tendensen med en ökande mängd utdrag som enskilda begär ur belastningsregistret medför en ökad risk för omotiverad registerkontroll, vilket kan leda till att personer som har avtjänat straff helt utestängs från arbetsmarknaden.

Riskerna för den personliga integriteteten vid registerkontroller samt medicinska kontroller har således relativt nyligen utretts. Det har även lämnats konkreta förslag till lagstiftning och andra åtgärder. Inget av de bägge förslagen har ännu skrinlagts, utan kan i dagsläget (maj 2016) fortfarande leda till lagstiftning. Vi fördjupar oss därför inte inom detta område.

[41] SOU 2014:48.

8.5 Arbetstagare och sociala medier

8.5.1 Företeelsen

Det förekommer att arbetsgivare regelbundet skannar av sociala medier för att bilda sig en uppfattning om vad arbetstagarna skriver om arbetsgivaren. Det har också blivit mycket vanligt att rekryterande chefer och rekryteringsföretag kontrollerar vad arbetssökande skrivit eller lagt upp på sociala medier.[42]

I media förekommer inte sällan rapporter om arbetsgivare som sagt upp arbetstagare på grund av bilder eller uttalanden som denne lagt ut på nätet. Ett känt exempel rörde tre personer som sades upp från ett it-företag efter uttalanden som de gjort på Facebook i syftet att visa stöd för en annan arbetstagare som arbetsgivaren redan tidigare hade sagt upp. Enligt uppgifter i media ska de tre personerna bl.a. ha skrivit: ”En sjua + AK47 gogogo. Jag är på semester” och ”As long as you shoot the fuckers and not the fuckees …”.[43] Fallet nådde Arbetsdomstolen men prövades inte där, eftersom parterna förliktes.[44]

I ett fall prövade Arbetsdomstolen uppsägningen av en bloggande polis. Polismannen, som hade bloggat under namnet ”Radiobilspolisen farbror blå”, sades upp av Polismyndigheten i Skåne bland annat pga. av vad man menade var olämpliga uttalanden på bloggen:[45]

> Såvitt avser hans syn på kvinnor har bl.a. framkommit att kvinnor som är tillräckligt snygga kan slippa böter, och att man på arbetstid har kunnat spana och ragga på snygga tjejer. Kvinnliga poliser har inte sällan förminskats till att antingen inte vara ”torra bakom öronen”, eller till att vara räddhågsna objekt som man möjligen kan ha sex med i polisbilen eller på personalfesten - och då kan man gärna vara flera män som delar på en kvinna. (…)Vidare har framkommit att han avskyr trafikpoliser vilka enligt honom bara ”djävlas med allmänheten”.

Arbetsdomstolen konstaterade emellertid att sådana följder av polismannens användning av yttrandefriheten som förtroendeförlust, förlorat anseende samt upprördhet och känslor av kränkning bland allmänheten och statsanställda inte i sig kan läggas till grund för att

[42] Anders Bolling, *Allt fler jobbgranskas på Facebook,* publicerad den 21 februari 2013 i Dagens Nyheter.
[43] Hans L. Olofsson, *Skrev på Facebook – tre avskedades*, publicerad den 2 september 2011 i Expressen.
[44] Elinor Torp, *Förlikning i Facebook-fallet*, publicerad den 23 augusti 2012 i Lag & Avtal.
[45] AD 2011 nr 74.

avsluta hans anställning hos polisen. I den utsträckning sådant kan ha förekommit ansåg Arbetsdomstolen att staten får tåla det. Det bör tilläggas att det i målet inte påståtts att polismannen utanför bloggen skulle ha uppvisat några av de beteenden som han hade beskrivit i bloggen.

I ett annat mål fann Arbetsdomstolen att uppsägningen av en rektor inte varit sakligt grundad.[46] Som skäl för uppsägningen hade arbetsgivaren uppgett rektorns agerande på sin privata Facebooksida. Arbetsgivaren åberopade att rektorn på sin Facebooksida hade lagt ut dels flera bilder med sexuellt innehåll, dels information om att han var med i ett antal grupper på Facebook med namn som hade anknytning till sex. En av bilderna visade rektorn utklädd till kvinna bärande peruk, en tröja med djup urringning och en kort kjol, med benen brett isär och en servett mellan benen. På en annan bild hade rektorn på sig en tröja, som skapats i ett elevprojekt i skolan, och som hade ett tryck i form av dels en bild av en kvinna i underkläder som står på alla fyra, dels texten NASA, vilket i detta sammanhang stod för ”National Anal Sex Association”.

Rektorn hade haft viss kontakt med elever på Facebook, bl.a. för att bestämma tid för möten och andra sammankomster. Arbetsdomstolen fann dock vid en samlad bedömning och intresseavvägning att rektorn inte enbart genom vad han lagt ut på sin Facebooksida hade gett skolan saklig grund för uppsägningen.

I ett annat fall fann Arbetsdomstolen att det förelåg laglig grund för att avskeda en lokförare som på ett internetforum, i e-post och i samtal till företagsledningen hade framfört hot samt kränkande och nedvärderande uttalanden som var riktade mot personer i ledningen.[47]

Justitiekanslern har i ett ärende prövat ett beslut av Utrikesdepartementet att i förtid avsluta en praktiktjänstgöring.[48] Praktikanten i fråga hade på sin arbetstid och från departementets datorer bloggat och därför enligt departementets uppfattning ägnat sig åt privat verksamhet – en verksamhet som har avsett opinionsbildning i kontroversiella politiska frågor. Praktikanten var partipolitiskt aktiv inom Sverigedemokraterna. Justitiekanslern fann att beslutet att avsluta praktiktjänstgöringen innebar både ett brott mot de arbetsrättsliga reglerna och en allvarlig kränkning av praktikantens grund-

[46] AD 2012 nr 25.
[47] AD 2011 nr 57.
[48] JK:s dnr 7068-06-21.

lagsfästa yttrandefrihet. Justitiekanslern nämner, som en av flera rättsliga utgångspunkter för sitt beslut, domen AD 2003 nr 5, och återger dess innehåll i följande ordalag.

> En myndighet kan i regel inte ingripa mot en anställd vid myndigheten för att den anställde genom att utnyttja sina grundlagsfästa fri- och rättigheter förorsakat störningar i verksamheten eller skadat myndighetens anseende och allmänhetens förtroende för myndigheten. Annat kan måhända gälla om det är fråga om en arbetstagare med en utpräglad förtroendeställning och direkt ansvar för myndighetens beslut eller i andra ytterlighetssituationer. Ett utrymme finns för att vidta åtgärder med anledning av allvarliga samarbetssvårigheter, även om dessa ytterst i viss mån kan ha sin grund i att en arbetstagare utnyttjat sina grundlagsfästa fri- och rättigheter. Givetvis bör en myndighet också kunna ingripa mot en anställd som inte utför sina arbetsuppgifter på ett riktigt sätt.

Ett annat fenomen som också rör arbetstagare och sociala medier, är att det blir allt vanligare att arbetsgivare använder sig av sociala medier för att informera eller kommunicera med arbetstagarna. Exempelvis har Facebook lanserat tjänsten *Facebook at Work*. Tanken är att arbetsgivarna i den nya tjänsten ska bygga upp sociala nätverk för sina arbetstagare.

8.5.2 Risker för den personliga integriteten

Om arbetsgivare inför anställningar eller under pågående anställningar tar för vana att systematiskt skanna av hela nätet och alla tillgängliga sociala medier, finns det på sikt en risk för att yttrandefriheten i arbetslivet undergrävs och att arbetstagarna mer eller mindre medvetet påverkas att uttrycka sig mindre fritt.

I en undersökning som Stockholms Handelskammare genomfört i samarbete med företaget Bisnode, uppger 25 procent av de medverkande företagen och organisationerna att de någon gång sorterat bort en kandidat med anledning av information de fått om kandidater via sökningar på nätet.[49]

När det gäller pågående anställningsförhållanden framgår det dock av Arbetsdomstolens praxis att det är endast är relativt allvarliga och hotfulla uttalanden som medfört att laglig grund för uppsägning har ansetts föreligga.

[49] *Så rekryterar företagen i framtiden*, Stockholms handelskammares analys 2014-02.

Systematisk skanning av nätet och sociala medier kan också leda till att arbetsgivaren sitter inne med en stor mängd överskottsinformation om arbetstagarna som den egentligen inte behöver för att kunna bedöma arbetstagarnas lämplighet och lojalitet.

En annan effekt kan bli att sökmotorerna och de företag som tillhandahåller sociala medier får en inverkan på anställningar och uppsägningar som en del arbetsgivare troligtvis inte är medvetna om. Effekten uppstår genom att det är sökmotorerna som sorterar och väljer ut vilka sökträffar som arbetsgivaren ska få upp i sin webbläsare. En annan effekt uppstår genom att det är de sociala medierna som med sina förinställningar kan förmå en arbetstagare att dela med sig av mer information än vad han eller hon kanske egentligen hade velat.

Det riskerar också att uppstå inlåsningseffekter genom att det kan vara svårt för exempelvis en arbetssökande att bli av med gamla texter och bilder på nätet som kan ha publicerats i sökandens ungdom utan en tanke på vilka konsekvenser detta kan ha flera år senare.

8.6 Kompetensdatabaser

8.6.1 Företeelsen

Många företag och organisationer har egna eller gemensamma kompetensdatabaser i syfte att sammanställa och dokumentera de anställdas kunskaper, erfarenheter och ibland även deras allmänna styrkor och svagheter.

Ett belysande exempel från offentlig sektor är Försvarsmaktens verksamhetsledningssystem PRIO, som innehåller funktioner för bland annat personal- och kompetenshantering. Försvarsmaktens hantering har relativt nyligen granskats av Datainspektionen.[50] Hanteringen av anställdas kompetenser i PRIO görs med hjälp av en kvalifikationskatalog där medarbetarna själva skattar sin kompetens inom ett i förväg avgränsat område. Medarbetarna registrerar uppgifter om vilka utbildningar och kurser de gått, vilka språkkunskaper de har samt vilka erfarenheter de har från olika arbetsområden inom Försvarsmakten. Skattningen görs i fördefinierade fält med graderade skalor, som antyder vilken nivå den anställde befinner sig på

[50] Datainspektionens beslut den 5 april 2013 i dnr 1610-2012.

inom respektive område. Uppgifterna som personalen registrerar om sig själva i PRIO matchas därefter mot de kravprofiler som gäller för olika befattningar inom Försvarsmakten.

Enligt Försvarsmakten är skattningen och den efterföljande matchningen i PRIO en förutsättning för att organisationen ska kunna bemannas effektivt och ändamålsenligt. Uppgifterna som personalen registrerat om sig själva i PRIO gör det också möjligt att identifiera behov av kompetensutveckling hos personalen. Uppgifterna ligger dessutom till grund för utvecklingssamtal.

Ett exempel på en gemensam kompetensdatabas i privat sektor är den s.k. *ID06 Kompetensdatabas* som har utvecklats av Sveriges Byggindustrier.[51] Syftet med databasen är att underlätta för såväl arbetsgivare som arbetstagare att hantera utbildningsbevis och samtidigt öka säkerheten på arbetsplatserna. Databasen ska i sin första version innehålla de enskilda arbetstagarnas utbildningsbevis inom arbetsmiljöområdet. De inlagda utbildningsbevisen kan komma från olika utbildningsföretag och kopplas i databasen till den enskilde arbetstagaren genom byggbranschens särskilda identitetskort, det s.k. ID06-kortet.

ID06 Kompetensdatabas ska göra det enkelt för arbetsgivare och arbetstagare att kontrollera giltiga utbildningsbevis på arbetsplatsen, med avseende bl.a. på de krav som ställs i Arbetsmiljöverkets föreskrifter om utbildning av arbetstagare. Det är i vissa situationer belagt med sanktionsavgift om rätt utbildningsbevis saknas eller är ogiltigt.

8.6.2 Risker för den personliga integriteten

Kompetensdatabaser kan ibland innehålla många olika uppgifter om de anställda som var för sig eller tillsammans är av integritetskänslig natur. Sådana kompetensdatabaser kan innebära en mycket ingående kartläggning av de anställda.

Det är inte ovanligt att arbetstagare är nyfikna på sina kollegor. Det finns därför en risk för nyfikenhetsläsning av uppgifter om kollegorna och därmed för obehörig åtkomst till uppgifterna i kompetensdatabasen, om denna saknar funktioner för att begränsa behörigheter och för kontroll av åtkomst i efterhand.

[51] Sveriges Byggindustrier är bransch- och arbetsgivarorganisation för bygg-, anläggnings- och specialföretag verksamma på den svenska byggmarknaden.

Eftersom en enskild arbetstagares kompetens och lämplighet i olika avseenden kan komma att ändras över tid, finns det också en risk för att vissa uppgifter i en kompetensdatabas snabbt kan bli inaktuella och oriktiga och till nackdel för arbetstagaren, om inte innehållet i databasen uppdateras och gallras regelbundet.

Beträffande kompetensdatabaser i offentlig verksamhet innebär det en risk att stora och integritetskänsliga uppgiftssamlingar om den enskilde arbetstagaren kan behöva lämnas ut som allmän handling, om de inte omfattas av sekretess. Den omständigheten var av betydelse i ett ärende där Datainspektionen ansåg att Försvarsmaktens personuppgiftsbehandling i en tidigare version av PRIO inte kunde anses som tillåten med stöd av en intresseavvägning enligt personuppgiftslagen.[52]

8.7 Bakgrundskontroller och kandidatdatabaser

8.7.1 Företeelserna

Bakgrundskontroller

Det har de senaste åren blivit allt vanligare att göra bakgrundskontroller i samband med rekryteringar, enligt den tidigare nämnda undersökningen från Stockholms Handelskammare och Bisnode.[53] Av de företag och organisationer som medverkade i undersökningen, svarade 29 procent att bakgrundskontroller görs för samtliga rekryteringar. Nästan alla medverkande kontrollerade de sökandes referenser. Därutöver kontrollerades vanligtvis även tidigare anställningar och utbildningshistorik. Många gör också sökningar på internet och i sociala medier som exempelvis bloggar, Twitter, Linkedin och Facebook. Av de medverkande företagen och organisationerna kontrollerade 26 procent även domar i brottmål och andra ärenden i domstol. Arbetsgivare i offentlig sektor utmärkte sig genom att lägga större vikt vid att undersöka utbildningshistorik, domar i brottmål och andra ärenden i domstol och använde sig även i större utsträckning av sökningar på internet, allt i jämförelse med arbetsgivare inom privat sektor.

[52] Datainspektionens beslut den 26 november 2010 i dnr 1454-2010.
[53] *Så rekryterar företagen i framtiden*, Stockholms handelskammares analys 2014-02.

Som konkret exempel på ingående bakgrundskontroller kan en verksamhet som var aktuellt i ett ärende hos Datainspektionen nämnas.[54] Det rörde sig om ett företag som utförde bakgrundskontroller på uppdrag av olika rekryterande arbetsgivare. Företaget inhämtade uppgifter om de sökande rörande: namn, bostadsadress, eventuella namnbyten, tidigare adresser, nationalitet, civilstånd, föräldrar, syskon, barn, nuvarande och tidigare fastighetsinnehav, inkomstuppgifter, registrerade skulder hos Kronofogdemyndigheten och Centrala studiemedelsnämnden, företagsengagemang, utbildningshistorik, körkort, värnpliktstjänstgöring, domar i brottmål och hos förvaltningsdomstolarna, förekomst på nätet och i sociala medier och i bloggar.

Det är också relativt vanligt med olika slags tester i samband med rekryteringar. Det kan röra sig om tester av sökandens personlighet, intelligens eller hälsa. Sådana tester är vanligare inom privat sektor än inom offentlig sektor. När frågan ställdes i den nämnda undersökningen om vilka slags bakgrundskontroller som företaget eller organisationen inte utför i dag, men skulle vilja utföra, uppgav 31 procent att de skulle vilja utföra alkohol- och drogtester för att ge ökad trygghet vid anställning.

På senare år har bakgrundskontroller också kunnat göras med hjälp av material från domar i brottmål som publiceras på nätet under skydd av s.k. frivilliga utgivningsbevis. Ett exempel på företag som tillhandahåller domar på nätet är Lexbase AB som i sin webbaserade tjänst mot en avgift tillhandahåller bl.a. domar i brottmål och tvistemål rörande personer och företag. Hantering av uppgifter som publiceras på nätet med skydd av utgivningsbevis, omfattas inte av reglerna i personuppgiftslagen. Det regelverk som avser att ge skydd för personuppgifter om lagöverträdelser blir därför inte tillämpligt här. Detta innebär att arbetsgivare enkelt kan genomföra bakgrundskontroller inför anställning eller kontroller av redan anställda. Utredningen Registerutdrag i arbetslivet konstaterar i sitt slutbetänkande att denna utveckling kan medföra att de integritetsskyddande åtgärder som föreslås i betänkandet skulle förlora mycket av sin betydelse.[55] Frågan om det rättsliga skyddet för den personliga integriteten är tillräckligt i databaser med utgivningsbevis, utreds för närvarande av Mediegrundlagskommittén.[56]

[54] Datainspektionens beslut den 30 november 2011 i dnr 1957-2010.
[55] SOU 2014:48, sid. 20 f.
[56] Ju 2014:17.

Kandidatdatabaser

De flesta rekryteringsföretag och även vissa arbetsgivare har s.k. kandidatdatabaser där sökande till en viss tjänst kan registrera sina uppgifter, lägga in sitt CV och ibland även göra webbaserade tester. Många sådana databaser är även öppna för intresseanmälningar inför framtida rekryteringar.

Datainspektionen genomförde år 2001 ett projekt för att kontrollera hur rekryteringsföretag hanterar uppgifter om de sökande.[57]

När Datainspektionen år 2011 granskade företag som erbjuder bakgrundskontroller, var det inget av företagen som hanterade uppgifter om de sökande i ett mer kvalificerat dokument- eller ärendehanteringssystem. Datainspektionen menade ändå att personuppgiftslagens omfattande s.k. hanteringsregler skulle tillämpas på hanteringen, och att undantagsbestämmelsen (den s.k. missbruksregeln) i 5 a § personuppgiftslagen således inte var aktuell. Som skäl för detta angavs att den aktuella hanteringen innebar en omfattande och systematisk kartläggning av den arbetssökande. Datainspektionen menade att det inte kan ha varit lagstiftarens intention att en sådan kartläggning av en individ skulle omfattas av undantaget för vardaglig behandling av personuppgifter. Två av företagen överklagade Datainspektionens beslut och fick till slut rätt i Högsta förvaltningsdomstolen som kom fram till att personuppgifterna hos de aktuella företagen var strukturerade endast på så sätt att de var listade i vad som utgör enkla digitala dokument i kalkyl- och ordbehandlingsprogram. Enligt domstolen hade datorteknikens fördelar således visserligen utnyttjats, men inte i fråga om strukturering i förhållande till manuell hantering. Mot den bakgrunden ansåg domstolen att personuppgifterna inte kunde anses ha strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter, att hanteringen därför omfattades av undantagsregeln i 5 a § första stycket personuppgiftslagen och att Datainspektionens och underrätternas avgöranden därför skulle undanröjas.

[57] Datainspektionens rapport 2002:3, *Behandling av personuppgifter hos rekryteringsföretag*.

8.7.2 Det skyddande regelverket

För hanteringen av personuppgifter i kandidatdatabaser gäller hanteringsreglerna i personuppgiftslagen.

I offentlig verksamhet gäller enligt offentlighets- och sekretesslagen sekretess i ärenden om anställning för uppgift som hänför sig till urvalstester, om det inte står klart att uppgiften kan röjas utan att den som uppgiften rör eller någon närstående till denne lider men.

Sekretess gäller också i ärenden om anställning av myndighetschef vid en förvaltningsmyndighet som lyder omedelbart under regeringen för uppgift som lämnar eller kan bidra till upplysning om en enskild kandidats identitet, om det inte står klart att uppgiften kan röjas utan att den enskilde lider men.

För myndigheter finns det en möjlighet att gallra allmänna handlingar, exempelvis får hos de flesta statliga myndigheter ansökningar avseende tjänst med tillhörande handlingar (ansökningshandlingar) gallras två år efter det att anställningsbeslutet vunnit laga kraft (Riksarkivets föreskrifter RA-FS 20014:1).

En s.k. säkerhetsprövning ska enligt säkerhetsskyddslagen (1996:627) göras angående personer som deltar i verksamhet som har betydelse för rikets säkerhet eller anlitas för uppgifter som är viktiga för skyddet mot terrorism. Säkerhetsprövningen kan bestå av registerkontroll och särskild personutredning. En särskild personutredning omfattar en undersökning av den kontrollerades ekonomiska förhållanden och ska i övrigt ha den omfattning som behövs. Den som säkerhetsprövningen gäller ska ha gett sitt samtycke innan registerkontroll och särskild personutredning får göras. Även i det nyligen framlagda betänkandet om ny säkerhetsskyddslag, föreslås att samtycke även i fortsättningen ska krävas innan registerkontroll och särskild personutredning får göras.[58]

8.7.3 Risker för den personliga integriteten

Både hos arbetsgivarna och hos rekryteringsföretagen kan det finnas ett intresse av att spara uppgifter om alla sökande i en avslutad rekrytering inför framtida rekryteringsbehov.

[58] Utredningens om säkerhetsskyddslagen betänkande *En ny säkerhetsskyddslag*, SOU 2015:25.

Det finns en risk för att detta görs utan att de sökande informeras och utan att deras samtycke till detta inhämtas.

I sin granskning av rekryteringsföretag, konstaterade Datainspektionen att det fanns brister i informationen till de sökande. I de flesta fall lämnades ingen information alls. Datainspektionen konstaterade också att de flesta av de granskade rekryteringsföretagen behöll uppgifterna längre tid än vad ändamålen med hanteringen krävde.

Datainspektionen fann också i sin granskning att vissa av rekryteringsföretagens personlighetstest redan år 2001 då granskningen genomfördes, var webbaserade och tillhandahölls av samarbetspartners till rekryteringsföretagen.

I dag är det troligen en ännu större andel av testerna inom arbetslivet som är webbaserade och tillhandahålls av någon annan är arbetsgivaren eller rekryteringsföretaget. Det finns därför en risk för att uppgifter om de sökande sprids utanför arbetsgivarens eller rekryteringsföretagets kontroll och att de sökande varken får tillräcklig information eller tillfrågas om sin inställning till denna spridning. Det finns också en risk för att uppgifterna kan komma att användas för ändamål som inte har något med själva rekryteringen att göra, exempelvis för att förbättra och utveckla testerna.

När det ställs närgångna och därmed integritetskänsliga frågor i testerna, är det inte självklart att arbetsgivare, rekryteringsföretag eller deras underleverantörer tänker på att integritetskänsliga uppgifter kräver ett starkare skydd. Det finns alltså en risk för att dessa uppgifter inte ges tillräckligt bra skydd.

Arbetsgivarverket har i sina kontakter med kommittén framfört att man anser att det finns ett integritetsproblem i och med att sekretess i rekryteringsförfaranden endast gäller för urvalstester och för uppgifter som kan avslöja sökandens identitet i ärenden om anställning av myndighetschefer.

8.8 Kameraövervakning

8.8.1 Företeelsen

I vissa branscher är kameraövervakning av arbetstagare mycket vanligt förekommande. Det kan röra sig om kameraövervakning både på platser dit allmänheten har tillträde och på platser dit allmänheten

inte har tillträde. Ett exempel på det förra är övervakning av butiksytor där både kunder och butikspersonal vistas. Ett exempel på det senare kan i samma butik vara övervakning av områden där bara personal får vistas såsom i lager eller pausutrymmen.

Den kameraövervakning som inbegriper arbetstagare kan i många fall egentligen vara inriktad på att övervaka eller kontrollera verksamhetens kunder, patienter eller brukare. Men eftersom arbetstagarna befinner sig i samma lokaler, träffas även de av arbetsgivarens övervakning.

År 2013 genomförde 19 av länsstyrelserna ett stort antal nationellt samordnade tillsynsinsatser inriktade på kameraövervakning i gallerier och köpcentrum och deras butiker.[59] Rapporten från tillsynsinsatserna inleds med konstaterandet att vi i dag blir övervakade såväl i utomhusmiljön som i inomhusmiljön, och att det blir allt färre platser i samhället som inte berörs av övervakning. I den samordnade tillsynen besöktes 116 gallerior och 693 butiker och övriga verksamheter. Efter butikerna var de flesta besökta verksamheterna restauranger och caféer. Av totalt 809 besök ledde 327 till anmärkningar. De vanligaste anmärkningarna var att det saknades överenskommelser med personalen om kameraövervakningen, att kameror var felriktade, att övervakning gjordes utanför butikslokal, att skyltningen var bristfällig eller obefintlig samt att anmälan eller tillstånd saknades.

Butiker, restauranger och caféer finns också med bland de arbetsplatser som pekades ut i Sveriges radios programserie om kameraövervakning av arbetsplatser hösten 2014.[60] Den mest omtalade bristen som nämns i programserien är olaglig användning av inspelningar från övervakningen. I programserien förekommer exempel på att inspelat material används för att kontrollera om anställda på ett lager står och pratar med varandra eller hur länge butikspersonal samtalar med kunderna. Även övervakningskameror på äldreboenden, som anhöriga sätter upp i sina släktingars rum eller lägenheter, tas i programserien upp som något som personalen kan uppleva som ett intrång.

Under år 2015 granskade Datainspektionen kameraövervakningen hos fyra butiker tillhörande olika detaljhandelskedjor. Myndigheten granskade specifikt övervakningskameror som var riktade mot platser som lager, lastkajer och liknande, alltså områden där kunder normalt

[59] Länsstyrelsernas rapport *Tillsyn av kameraövervakning över gallerior/köpcentrum och dess verksamheter 2013*.

[60] Övervakad på jobbet, Sveriges radio, 2014, www.sverigesradio.se

sett inte befinner sig. I besluten riktade Datainspektionen kritik mot samtliga fyra butiker för hur dessa kameraövervakade lagerutrymmen, personalingångar och lastkajer och förelade butikerna att se till att sådana utrymmen enbart övervakas under tider då personal inte ska befinna sig i utrymmena.[61] Butikerna kritiserades även för att de inte tillräckligt tydligt informerade om den kameraövervakning som förekommer.

På senare år har utrustningar för kameraövervakning blivit mycket bättre, billigare och enklare att använda. Exempelvis kan inspelningar överföras över internet och enkelt visas på en dator eller smart enhet. Bildhanteringen kan också kompletteras med funktioner för ansiktsigenkänning. Kameraövervakning som egen företeelse behandlas närmare i kapitel 20.

För närvarande pågår en översyn av kameraövervakningslagen (2013:460) i Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd.[62] Utredaren ska enligt direktiven bl.a. ta ställning till om integritetsskyddet på vissa platser dit allmänheten inte har tillträde, till exempel arbetsplatser och skolor, behöver förbättras. Uppdraget ska redovisas senast den 28 februari 2017.[63]

8.8.2 Det skyddande regelverket

Enligt kameraövervakningslagen krävs som huvudregel tillstånd till kameraövervakning för att en övervakningskamera ska få vara uppsatt så att den kan riktas mot en plats dit allmänheten har tillträde.

I vissa fall räcker det dock med att den som vill kameraövervaka gör en anmälan om detta till länsstyrelsen. Till exempel får alla allmänna utrymmen i en butik kameraövervakas efter att en anmälan har gjorts, under förutsättning att övervakningen görs i syfte att förebygga, avslöja eller utreda brott.

Kameraövervakning av en plats dit allmänheten *inte* har tillträde får bedrivas utan tillstånd. Övervakning får då bedrivas med samtycke från dem som övervakas, eller om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller andra berättigade ändamål, och övervakningsintresset väger tyngre än den

[61] Datainspektionen beslut den 16 december 2015 i ärendena 340-2015, 342-2015, 347-2015 och 351-2015.
[62] Ju 2015:14.
[63] Dir. 2015:125.

enskildes intresse av att inte bli övervakad. Det ska även beaktas hur övervakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet används och vilket område som ska övervakas.

När det gäller platser dit allmänheten inte har tillträde, finns det ingen skyldighet för arbetsgivaren att anmäla kameraövervakningen till någon myndighet.

Vidare ska enligt 30 § kameraövervakningslagen den som bedriver kameraövervakning vidta lämpliga tekniska och organisatoriska åtgärder för att skydda det upptagna bild- och ljudmaterialet. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,
3. de särskilda risker som finns med behandlingen av materialet, och
4. hur pass känsligt materialet är.

8.8.3 Risker för den personliga integriteten

Kameraövervakning av arbetsplatser och arbetstagare är i vissa branscher mycket vanligt förekommande, företrädesvis i olika serviceyrken, i transportarbeten och vid arbete på lager.

Av såväl länsstyrelsernas ovan nämnda rapport som av uppgifter i media framgår att det i dessa branscher finns allvarliga brister i tillämpningen av kameraövervakningslagens integritetsskyddande regler.

Det kan således konstateras att många arbetstagare i landet övervakas för ändamål och på ett sätt som inte är förenligt med gällande lagstiftning. Om den tilltagande teknikutvecklingen och den nedåtgående prisutvecklingen för kameraövervakningsutrustning håller i sig, finns dessutom en risk för att de redan konstaterade bristerna kommer att öka i takt med att allt fler övervakningskameror installeras på arbetsplatserna.

Det finns en risk att arbetsgivare felaktigt tror sig kunna grunda kameraövervakningen på arbetstagarnas samtycke. I ett tillsynsärende hos Datainspektionen grundade en arbetsgivare kameraövervakningen just på arbetstagarnas samtycke, med hänvisning till att arbetstagare som upplevde obehag med övervakningen hade

”möjlighet att ta kontakt med arbetsledningen för eventuellt byte av arbetsplats”.[64] Enligt Datainspektionen utgjorde detta inte ett sådant reellt alternativ till kameraövervakning som medförde att samtycke kunde anses föreligga.

Risken är också stor att material från kameraövervakning kan komma att användas för andra ändamål än de som ursprungligen föranledde installationen av övervakningskamerorna.[65] Som exempel kan nämnas ett ärende hos Datainspektionen där material från kameraövervakningen i en skola användes för att kontrollera hur den kontrakterade städentreprenören utförde sitt arbete på kvällarna. Kamerorna hade egentligen satts upp för att förhindra skadegörelse, inbrott och stölder.

Av Sveriges Radios rapportering framgår också att länsstyrelserna vanligtvis endast förmår utföra enstaka stickprovskontroller av arbetsgivarnas tillämpning.

Tillsyn av kameraövervakning på platser dit allmänheten *inte* har tillträde görs av Datainspektionen. Det är uppenbart att en så liten myndighet med många andra arbetsuppgifter inte kan göra annat än ett fåtal stickprovskontroller när det gäller en så pass omfattande och nationellt spridd företeelse som kameraövervakning.

När det gäller kameraövervakning av platser dit allmänheten har tillträde, krävs antingen ett tillstånd från eller en anmälan till länsstyrelsen. Detta ger länsstyrelserna möjlighet både att hitta arbetsplatser som kameraövervakas och att bilda sig en uppfattning om hur omfattande den sammanlagda kameraövervakningen är på landets arbetsplatser. Hur mycket tillsyn av övervakningskameror som länsstyrelserna kan ägna sig åt, är i slutändan en kostnads- och prioriteringsfråga.

När det gäller kameraövervakning av platser dit allmänheten *inte* har tillträde, finns det inget sätt för tillsynsmyndigheten Datainspektionen att få veta att kameraövervakning förekommer, utom genom att ställa frågan till varje arbetsgivare. Datainspektionens tillsyn av området försvåras därmed, jämfört med de möjligheter som länsstyrelserna har eftersom dessa åtminstone får in anmälningar (eller ska få in dem) och därmed kan få veta var kameraövervakning bedrivs och kontrollera den.

[64] Datainspektionens beslut den 3 december 2014 i dnr 1652-2014.
[65] Datainspektionens beslut den 29 oktober 2009 i dnr 476-2009.

8.9 Företagshälsovård

8.9.1 Företeelsen

Det är mycket vanligt att arbetsgivare anlitar ett vårdföretag för att tillhandahålla företagshälsovårdstjänster till sina arbetstagare, bestående i hälso- och sjukvård. I en sådan situation är vårdgivaren själv ansvarig för den hantering av uppgifter om arbetstagarna som måste göras för att dessa ska kunna ges hälso- och sjukvård.

Det förekommer också att arbetsgivaren anlitar samma vårdgivare för att även utföra arbetsuppgifter av rent personaladministrativ natur. Det kan exempelvis röra sig om att för arbetsgivarens räkning ta emot sjuk- och friskanmälningar eller anmälningar om frånvaro på grund av vård av barn. Arbetstagarna instrueras då att göra dessa anmälningar till vårdgivaren. När vårdgivaren tagit emot anmälningarna från arbetstagarna, vidarebefordrar den uppgifterna till arbetsgivaren. Vårdgivaren utför då ingen hälso- och sjukvård. I en sådan situation är det arbetsgivaren som är ansvarig för vårdgivarens hantering av uppgifter om arbetstagarna. Vårdgivaren utför i denna situation inget självständigt uppdrag, utan hanterar endast uppgifter för arbetsgivarens räkning och ändamål. Vårdgivaren är personuppgiftsbiträde till arbetsgivaren för hanteringen av uppgifter för den här typen av personaladministrativa ändamål.

Datainspektionen har i några ärenden granskat ansvarsförhållandena i situationer då vårdgivare varit kontrakterade för att tillhandahålla både företagshälsovård och samtidigt personaladministrativa tjänster.[66]

Företeelsen var nyligen föremål för en tvist i Arbetsdomstolen.[67] I målet var frågan om en arbetsgivare som anlitat ett privat hälso- och sjukvårdsföretag för att administrera sjuk- och friskanmälningar. Fackförbundet menade att arbetsgivaren bröt mot personuppgiftslagen när den behandlade känsliga personuppgifter om hälsa som den fick från vårdgivaren. Bland annat skickade vårdgivaren uppgifter till arbetsgivaren om att den sjuka arbetstagaren inte svarar i telefon när vårdgivaren ringer på tredje sjukdagen. Det ska enligt stämningsansökan också ha förekommit att uppgifter om sjukdom och diagnos

[66] Datainspektionens beslut den 14 augusti 2012 i dnr 1176-2011, 1177-2011, 1179-2011, 1180-2011, 1181-2011, 1182-2011 och beslutet den 31 juli 2012 i dnr 455-2012.

[67] Arbetsdomstolens mål A 229/14. Målet avgjordes inte genom dom, utan parterna förliktes och målet avskrevs.

skickades från vårdgivaren till arbetsgivaren. Förbundet hade yrkat skadestånd för brott mot personuppgiftslagen till två av sina berörda medlemmar.

För arbetsgivaren kan det många gånger te sig lämpligt att låta en och samma privata vårdgivare tillhandahålla tjänster för såväl företagshälsovård som personaladministration. Vårdgivaren kan då exempelvis när den får in en sjukanmälan från en arbetstagare, passa på att ställa frågor och ge råd om hur arbetstagaren så snabbt som möjligt ska tillfriskna och kunna återgå i arbete. Vidare har en vårdgivare oftast bättre förutsättningar för att tidigt uppfatta om det bakom en sjukanmälan döljer sig en mer djupgående problematik där det behövs andra eller mer omfattande insatser från företagshälsovården eller arbetsgivaren.

8.9.2 Det skyddande regelverket

För vårdgivarens hantering av personuppgifter för personaladministrativa ändamål för arbetsgivarens räkning, gäller personuppgiftslagens bestämmelser.

När vårdgivaren tillhandahåller företagshälsovårdstjänster och utför hälso- och sjukvård gäller patientdatalagens (2008:355) bestämmelser. Vidare råder inom sådan verksamhet tystnadsplikt enligt patientsäkerhetslagen (2010:659) för uppgifter om en enskilds hälsotillstånd eller andra personliga förhållanden.

8.9.3 Risker för den personliga integriteten

När en vårdgivare ska tillhandahålla både hälso- och sjukvård och personaladministrativa tjänster, finns det en risk för att samtliga involverade parter blandar ihop vårdgivarens olika roller.

Vårdgivaren kan komma att vidareförmedla uppgifter till arbetsgivaren som noga taget hör till hälso- och sjukvårdsdelen av vårdgivarens uppdrag och som egentligen omfattas av tystnadsplikt även i förhållande till arbetsgivaren.

Arbetstagaren kan invaggas i tron att vårdgivaren agerar enbart inom sitt uppdrag som företagshälsovård, och kan då komma att lämna sådana hälsouppgifter som arbetstagaren aldrig skulle ha avslöjat direkt för arbetsgivaren, trots att uppgifterna faktiskt hamnar just hos arbetsgivaren till slut.

Om arbetstagaren inte känner sig säker på vilka uppgifter som vårdgivaren kommer att vidarebefordra till arbetsgivaren, finns det också en risk för att han eller hon kommer att avslöja för litet om sitt hälsotillstånd och undanhåller uppgifter som hade varit relevanta och nödvändiga för att vårdgivaren ska kunna ge adekvata råd och eventuella behandlingar.

8.10 Kommitténs samlade bedömning av området

Ett tydligt och problematiskt fenomen som gäller generellt inom arbetslivet, är risken för ändamålsglidningar när arbetsgivare digitalt hanterar uppgifter om arbetstagare. Det kan också konstateras att Datainspektionens praxis har varit relativt tillåtande inför ändamålsglidningar inom arbetslivet.

Positionering samt annan övervakning av aktiviteter och beteenden

Arbetstagare avsätter allt fler och mer detaljerade elektroniska spår, samtidigt som utrustning och system för att övervaka och kontrollera blir allt billigare och enklare att använda.

En annan del av utvecklingen är att uppgifter om arbetstagare i allt större utsträckning hamnar hos externa leverantörer, inte sällan i molntjänster, som kan innebära en omfattande och svårkontrollerad spridning, lagring och vidareanvändning av uppgifterna. Flera led i den hanteringen görs många gånger utan vare sig arbetsgivarens eller arbetstagarnas kännedom.

Arbetstagaras möjligheter att påverka hanteringen är begränsade redan initialt, pga. arbetsledningsrätten, men försämras ytterligare av bristen på kunskap om hanteringen.

Det sagda, i kombinationen med faran för ändamålsglidningar i arbetslivet, medför att kommittén anser att det finns allvarliga risker för den personliga integriteten när arbetsgivare använder sig av positionering och annan övervakning för att kontrollera arbetstagarnas aktiviteter och beteenden på arbetet.

Samtidigt måste beaktas att arbetsgivaren för att leda, organisera och följa upp arbetet kan behöva relativt detaljerade uppgifter om var arbetstagarna befinner sig, hur de använder sig av arbetsgivarens utrustning och vad de ägnar sin arbetstid åt.

Sociala medier

När arbetsgivare skannar av sociala medier för att bilda sig en uppfattning om vad arbetstagarna gör på nätet, innebär det att arbetsgivaren träder in på en arena som den enskilde vanligen kan betrakta som privat snarare än arbetsrelaterad. Emellertid finns det oftast möjligheter för arbetstagare att begränsa åtkomsten till uttalanden som skulle kunna uppfattas som känsliga eller kontroversiella i förhållande till arbetsgivaren. Därför anser kommittén att arbetsgivares granskningar av vad arbetstagare skriver på sociala medier, innebär en viss risk för den personliga integriteten.

Samtidigt måste anses rimligt att arbetsgivare i sin omvärldsbevakning, inhämtar information från många olika källor, däribland publik information i sociala medier.

Kompetensdatabaser och bakgrundskontroller

Både kompetensdatabaser och utförande av bakgrundskontroller, kan innebära att många olika slags uppgifter om arbetstagarna hanteras. Ibland kan redan enskilda uppgifter vara integritetskänsliga, medan det i andra situationer är sammanställningar av många uppgifter som tillsammans ger en närgången och detaljerad bild av arbetstagaren. Samtidigt är det troligen inte vanligt förekommande med omfattande och detaljerade kompetensdatabaser och bakgrundskontroller. Vidare är spridningen av uppgifterna sannolikt begränsad, liksom många gånger åtkomsten till dem. Kommittén anser därför att kompetensdatabaser och bakgrundskontroller innebär en viss risk för den personliga integriteten.

Samtidigt måste beaktas att arbetsgivare kan behöva dokumentera arbetstagarnas kompetenser och genomföra bakgrundskontroller för att effektivt kunna leda och fördela arbetet och så långt som möjligt undvika felrekryteringar som både kan bli kostsamma och ha negativa effekter för andra arbetstagare hos arbetsgivaren.

Kameraövervakning

Kameraövervakning omfattar allt fler arbetstagare samtidigt som det finns granskningar som visar att många arbetsgivare tillämpar den skyddande lagstiftningen på ett felaktigt sätt. Vidare finns det rapporter om att bilder från kameraövervakning använts för helt andra ändamål än dem för vilka kamerorna installerades. Kommittén anser därför att kameraövervakning på arbetsplatser innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste beaktas att kameraövervakning kan medföra direkta fördelar för enskilda arbetstagare, främst när säkerheten på arbetsplatsen förbättras av övervakningen.

Företagshälsovård

När en vårdgivare ska tillhandahålla både hälso- och sjukvård och personaladministrativa tjänster, kan det uppstå en sammanblandning av vårdgivarens olika roller, som kan få till följd att arbetsgivaren får ta del av uppgifter som hör till hälso- och sjukvårdsdelen av vårdgivarens uppdrag och som omfattas av tystnadsplikt även i förhållande till arbetsgivaren. Det finns emellertid ett tydligt regelverk både för tystnadsplikt gentemot arbetsgivare i dessa situationer, och för hur en vårdgivare får hantera personuppgifter (patientdatalagen). Kommittén anser att det finns en viss risk för den personliga integriteten när vårdgivare ska tillhandahålla såväl hälso- och sjukvård som personaladministrativa tjänster.

Samtidigt kan det finnas fördelar även för den enskilde arbetstagaren om både företagshälsovård och personaladministrativa tjänster tillhandahålls av samma företag, i form av snabbare och enklare kontakt och hjälp vid sjukfall.

Personuppgiftslagen och tillsynen

I kommitténs möten med arbetsmarknadens parter har vidare framkommit att såväl fackliga organisationer som arbetsgivarorganisationer anser att personuppgiftslagen är svår att tillämpa på arbetslivsområdet. Det har också gjorts gällande att Datainspektionens vägledning, i den mån den efterfrågats, inte alltid är tillräckligt tydlig för att ge parterna den hjälp som de behöver.

Brister i kunskap och i den vägledning som ges, kan vara en del av förklaringen till att personuppgiftslagen mycket sällan används som sanktionsmedel av arbetstagarna eller deras organisationer. Det är anmärkningsvärt att det, trots den enorma tekniska utvecklingen, inte har uppkommit särskilt många tvister om personlig integritet inom arbetslivet i samband med användning av informationsteknik.

I likhet med vad som konstaterades i betänkandet *Integritetsskydd i arbetslivet*[68], kan det fortfarande i dag sägas att bestämmelserna i personuppgiftslagen inte förefaller ha fått det genomslag på arbetslivets område som man hade kunnat förvänta sig. I betänkandet kunde vid en internationell jämförelse också konstateras att de finländska och norska motsvarigheterna till personuppgiftslagen haft ett större genomslag på arbetslivets område, utan att några avgörande skillnader finns mellan ländernas dataskyddsrättsliga och arbetsrättsliga lagstiftning. Förklaringen antogs vara att aktiviteten helt enkelt varit högre i dessa grannländer och att man tidigare än i Sverige hade förstått att utnyttja dataskyddsreglerna på arbetslivets område.[69]

Ett särskilt regelverk för integritetsskydd i arbetslivet skulle kunna medföra att det blir lättare för parterna att förstå hur regelverket ska tillämpas på förhållandena i arbetslivet, och därmed kanske skulle kunna leda till att reglerna börjar användas oftare i parternas förhandlingar och tvister.

Kommittén kan också konstatera att Datainspektionens tillsyn görs av enstaka företeelser, men att tillsynen inte leder till att myndigheten får en övergripande uppfattning av hur omfattande övervakningen faktiskt är av landets arbetstagare och i vilka former den bedrivs.

[68] SOU 2009:44.
[69] SOU 2009:44.

Beträffande kameraövervakning bedömer vi att det inte förefaller troligt att dagens tillsynsinsatser ensamma skulle kunna åstadkomma någon generell förbättring av arbetsgivarnas tillämpning.

Kommittén kan också konstatera att Datainspektionen inte används av parterna i den utsträckning som faktiskt vore möjligt – exempelvis skulle myndighetens bedömning av olika övervakningsåtgärder kunna inhämtas vid MBL-förhandlingar i samband med införandet av nya system som kan innebära övervakning eller inför tecknandet av nya kollektivavtal.

Sammanfattning

Det är tydligt att ny teknik och nya arbetssätt ökar möjligheterna att kartlägga och övervaka arbetstagare på ett mycket närgånget och detaljerat sätt.

Ny teknik i kombination med nya arbetssätt innebär också risk för en ökande och oönskad sammanblandning av arbetstagarnas privatliv och arbetsliv.

Till detta kommer att den ökande användningen av övervakningstekniker i samhället i stort, träffar arbetstagare även när den egentliga avsikten med övervakningen inte är att kontrollera arbetstagarna, utan verksamhetens kunder, patienter eller brukare. Även när detta görs oavsiktligen, bidrar det ändå till att öka övervakningen av arbetstagarna. Sådan övervakning omfattar särskilt vissa yrken, t.ex. säljare i butik, vårdbiträden samt personal i restauranger och caféer, vilka kännetecknas bl.a. av att de sysselsätter en betydligt högre andel kvinnor än män. Å andra sidan är andra, mer direkt övervakade yrken vanligare för män, t.ex. lastbils- och långtradarförare samt lagerarbetare. Dessa yrken sysselsätter dock färre arbetstagare än i de tidigare nämnda kvinnodominerade yrkesgrupperna.[70]

De ökade möjligheterna till detaljerad kontroll, kartläggning och övervakning i realtid riskerar att förskjuta styrkeförhållandena inom arbetslivet och att försvaga arbetstagarnas ställning.[71]

---

[70] Enligt Statistiska centralbyråns yrkesregister med yrkesstatistik (december 2015).

[71] Norska Datatilsynet uttrycker detta i följande ordalag: ”Den totale mengden av kontrolltiltak og registreringer kan også gjøre at balansen mellom partene i arbeidslivet forskyves ytterligere. Arbeidsgiveren vet mye om hver og enkelt av oss, men vi vet ikke nødvendigvis hva som registreres, hvem som ser hva, og hva opplysningene kan og skal brukes til” Datatilsynets rapport ”*En vanlig dag på jobb” Arbeidshverdagens elektroniske spor*, oktober 2012.

Samtidigt är det viktigt att beakta att arbetsgivare har en rätt att vidta sådana åtgärder som är rimliga och som faller inom rätten att leda och fördela arbetet. Arbetsgivaren har också en skyldighet att upprätthålla säkerheten för både arbetstagare och utrustning. Effektiva och säkra arbetsplatser har många fördelar även ur den enskilde arbetstagarens perspektiv.

Digitaliseringen i samhället innebär att stora mängder uppgifter om arbetstagare kommer att sparas under oöverskådlig tid och att uppgifterna lätt kan spridas, bearbetas och vara tillgängliga för många. Det är inte förvånande att många arbetsgivare använder sig av olika kontroll- och övervakningsfunktioner för att minska riskerna för felaktiga beslut i verksamheten och vid rekrytering. Samtidigt riskerar denna utveckling att leda till en exkludering från arbetslivet av allt fler individer.

9 Hälso- och sjukvård och välfärdsteknik inom socialtjänst

Kommitténs bedömning: Det föreligger allvarliga risker för den personliga integriteten i samband med hantering av personuppgifter inom hälso- och sjukvården och i samband med socialtjänstens användning av välfärdsteknik.

9.1 Inledning

9.1.1 Beskrivning av området

I detta kapitel beskriver kommittén några av de integritetsrisker som finns inom hälso- och sjukvården och socialtjänsten. När det gäller socialtjänsten kommer vi i endast att beskriva de risker som är förenade med viss användning av s.k. välfärdsteknik (begreppet förklaras i avsnitt 9.6).

För att den enskilde individen ska kunna erbjudas god vård och omsorg måste de ansvariga verksamheterna dokumentera och i övrigt hantera information om individen och hans eller hennes behov och om de insatser som planeras och genomförs. Även resultaten för individen måste dokumenteras och följas upp. För att verksamheten ska kunna utveckla sin kvalitet behöver resultaten också kunna följas upp.

När en person får insatser inom hälso- och sjukvården och socialtjänsten är dokumentationen en integrerad del av analys, bedömning och genomförande av insatsen. Personalen tar del av nödvändiga uppgifter om individen före mötet med honom eller henne samt även under och efter arbetets genomförande. Uppgifter kan behöva doku-

menteras och på olika sätt användas under hela detta förlopp. Informationssystem kan också fungera som beslutsstöd direkt i arbetssituationen.

Dokumentationen i hälso- och sjukvården och socialtjänsten är utan tvekan av mer integritetskänslig karaktär än vad information i många andra sammanhang är. Det handlar i princip uteslutande om uppgifter som rör människors hälsa och livssituation. Hos landets alla vårdgivare (offentliga eller privata vårdgivare) lagras uppgifter elektroniskt om större delen av befolkningen. Uppgifter om många av landets invånare hanteras också av dem som bedriver socialtjänst.

Vid ett besök i vården hanteras patienternas uppgifter även för andra syften än den hantering som behövs för att kunna ge den vård som behövs i det enskilda fallet. Exempelvis hamnar vissa uppgifter i kvalitetsregister med anknytning till hälso- och sjukvården. Beroende på vilka vårdinsatser som har getts, måste uppgifter också skickas av vårdgivaren till något av Socialstyrelsens hälsodataregister som officiell statistik.

Om patienten vid besöket i vården får ett läkemedel förskrivet, så sänder vårdgivaren receptet elektroniskt till det centrala receptregistret hos eHälsomyndigheten. Behörig personal på alla öppenvårdsapotek i landet har tillgång till detta register.

Vidare kan uppgifter om sjukdom och erhållen vård ibland komma att hanteras och läsas i helt andra syften. Exempelvis kan uppgifter komma att användas i ett forskningsprojekt, hanteras i en biobank eller skickas till ett centralt hälsodataregister.

Viss hantering av uppgifter får göras oavsett patientens inställning, dvs. att något samtycke inte är nödvändigt och att patienten varken kan hindra eller påverka att eller hur uppgifter behandlas. Vanligen finns dock ett lagkrav på att patienterna ska informeras om att och hur deras uppgifter hanteras.

9.1.2 Regelverk och tillsyn

Hälso- och sjukvården

Hanteringen av personuppgifter som förekommer med anledning av ett besök i vården regleras av olika författningar, i huvudsak följande:

- inom vård och kvalitetsutveckling regleras hanteringen i patientdatalagen (2008:355),
- hur uppgifter om ordinerade läkemedel får hanteras regleras i lagen (1996:1196) om receptregister, lagen (2005:258) om läkemedelsförteckning och apoteksdatalagen (2009:367),
- när uppgifter om blod- och vävnadsprov hanteras, regleras det av lagen (2002:297) om biobanker i hälso- och sjukvården m.m. och personuppgiftslagen,
- generellt inom offentlig verksamhet gäller offentlighets- och sekretesslagen (2009:400), för privata vårdgivare finns bestämmelserna om tystnadsplikt i patientsäkerhetslagen (2010:659),
- vårdgivarens övergripande ansvar för kvaliteten i vården regleras i hälso- och sjukvårdslagen (1982:763), patientsäkerhetslagen och i Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete.

Informationshanteringen inom hälso- och sjukvården ska enligt 1 kap. 2 § patientdatalagen vara organiserad så att den tillgodoser patientsäkerhet, god kvalitet samt främjar kostnadseffektivitet. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem.

Socialtjänsten

Socialtjänstens hantering av personuppgifter regleras av personuppgiftslagen, av lagen (2001:454) om behandling av personuppgifter inom socialtjänsten och av förordningen (2001:637) om behandling av personuppgifter i socialtjänsten.

De regler som styr handläggning och dokumentation i socialtjänsten återfinns framför allt i förvaltningslagen (1986:223), socialtjänstlagen (2001:453) och i lagarna med särskilda bestämmelser vid vård av unga (1990:52), om vård av missbrukare (1988:870) i vissa fall, samt om stöd och service till vissa funktionshindrade (1993:387).

Därutöver har även lagstiftning som offentlighets- och sekretesslagen, arkivlagen (1990:782) och tryckfrihetsförordningen betydelse för socialtjänstens informationshantering.

Tillsyn m.m.

I första hand två tillsynsmyndigheter kontrollerar hantering av personuppgifter inom hälso- och sjukvården och socialtjänsten: Datainspektionen (med inriktning på integritetsskydd) och Inspektionen för vård och omsorg (med inriktning på patient- och brukarsäkerhet).

Vidare ska det i varje kommun och landsting finnas en eller flera patientnämnder med uppgift att stödja och hjälpa patienter inom all offentligt finansierad hälso- och sjukvård och tandvård. Patientnämnderna ska utifrån synpunkter och klagomål stödja och hjälpa enskilda patienter och bidra till kvalitetsutveckling och hög patientsäkerhet i hälso- och sjukvården genom att hjälpa patienter att få den information patienterna behöver för att kunna ta till vara sina intressen i hälso- och sjukvården, främja kontakterna mellan patienter och vårdpersonal, hjälpa patienter att vända sig till rätt myndighet, samt rapportera iakttagelser och avvikelser av betydelse för patienterna till vårdgivare och vårdenheter. (jfr lagen [1998:1656] om patientnämndsverksamhet m.m.)

Därtill utövar Riksdagens ombudsmän (Justitieombudsmannen) och i viss mån Justitiekanslern tillsyn över den allmänna hälso- och sjukvården och forskningen, och polis och åklagare utreder misstänkta brott.

Den enskilde som anser att hennes eller hans uppgifter hanterats på ett felaktigt sätt, t.ex. genom att uppgifter har spridits till anställda som inte behöver dem för att kunna utföra sitt arbete, och som därmed anser att det gjorts ett otillbörligt intrång i hennes eller hans personliga integritet, kan således välja mellan flera olika myndigheter att vända sig till med ett klagomål. Förutom till vårdgivaren själv kan klagomål anmälas till patientnämnden, Datainspektionen, Justitieombudsmannen eller till polis och åklagare. Vidare finns det en möjlighet för patienten att begära skadestånd vid allmän domstol för den ideella skada som hon eller han anser sig ha lidit på grund av integritetsintrång.

9.2 Allmänt om hanteringen av personuppgifter inom hälso- och sjukvården

9.2.1 Informationshantering i hälso- och sjukvården

Hälso- och sjukvården har alltsedan patientdatalagen trädde i kraft 2008 genomgått stora strukturförändringar varav en av de mest markanta är ökningen av andelen privata vårdgivare. Enligt *Utredningen om rätt information i vård och omsorg*[1] ökade landstingens köp av vårdtjänster från privata leverantörer från 18 miljarder kronor till cirka 32 miljarder kronor under perioden 2006–2012. Bara i Stockholms läns landsting finns, förutom offentliga vårdleverantörer, omkring 3 000 privata verksamheter som bedriver hälso- och sjukvård (inklusive företagare på nationella taxan och inom tandvården). Även om mångfalden av privata och offentliga vårdgivare skiljer sig åt i olika delar av landet pekar den sammantagna utvecklingen på att mångfalden ökar och att de privata vårdgivarna blir fler. Samtidigt är det, i allt väsentligt, kommuner och landsting som finansierar såväl de offentliga som de privata vårdgivarnas verksamhet. Tillsammans med det ökade antalet vårdgivare har även specialiseringen inom hälso- och sjukvården ökat.

Efter avregleringen av apoteksmarknaden består apotekssektorn i dag av ett 25-tal olika aktörer som bedriver cirka 1 300 apotek.[2]

Utvecklingen har medfört att det ofta är fler aktörer än tidigare inblandade i vården av samma patient. För patienter som är i behov av koordinerade insatser från primärvården och specialistvården är det i dag snarare regel än undantag att samarbetet inbegriper två eller fler självständiga vårdgivare. Bara i en sjukhusbyggnad kan ett flertal olika vårdgivare vara verksamma som samarbetar i vården av patienterna. Ett sådant samarbete pågår ofta utan att patienten själv är medveten om att vården ges av olika vårdgivare. Ett annat exempel på detta är den mångfald av vårdgivare inom ambulanssjukvården som exempelvis finns i Stockholms läns landsting. Det är i dag inte ovanligt att den privata vårdgivare som står för insatserna i ambulansen assisteras av en akutbil med läkare eller sjuksköterskor från en annan privat vårdgivare. Utvecklingen ser i stort likadan ut i den

[1] Utredningens om rätt information i vård och omsorg betänkande *Rätt information på rätt plats i rätt tid*, SOU 2014:23, s. 110.
[2] E-hälsokommitténs betänkande *Nästa fas i e-hälsoarbetet*, SOU 2015:32, s. 161.

landstingsfinansierade och i den kommunalt finansierade hälso- och sjukvården. Denna mångfald av olika driftsformer ställer förstås krav på effektiv samverkan och ändamålsenligt informationsöverföring.

Även olika krav på samverkan mellan kommuner och landsting innebär att det måste finnas former för ändamålsenlig och säker informationsöverföring.

9.2.2 Hur ser informationshanteringen ut i dag?

I dag börjar det bli missvisande att över huvud taget tala om ”patientjournaler” som bärare av personuppgifter i hälso- och sjukvården. Snarare rör det sig i dag om lagrade personuppgifter som presenteras i olika former för olika aktörer inom vården. Svensk sjukvårds-it består av ett mycket stort antal system och tjänster som lagrar och distribuerar patientinformation.

Ett annat område som är under utveckling är användningen av olika former av it-stöd i vårdarbetet.

Beslutsstöd kan lite förenklat beskrivas som ett datorstött system som baserat på kunskapsstöd kan ge patientspecifika råd och rekommendationer kring prevention, prognos, diagnostik, behandling och uppföljning för läkare, annan hälso- och sjukvårdspersonal och patienterna själva. *Kunskapsstöd* är en datorbaserad kunskapskälla som presenterar kunskap men utan någon direkt koppling till specifik patientinformation. Kunskapen rör ett visst kliniskt område och innehåller till exempel vägledning, rekommendationer, termdefinitioner och förslag på indikatorer.[3]

E-hälsokommittén redovisar i sitt betänkande[4] en kartläggning som e-hälsomyndigheten gjort avseende beslutsstöd. I kartläggningen konstateras att i Sverige är system för läkemedelshantering den vanligaste typen av besluts- och kunskapsstöd i hälso- och sjukvården. En möjlig förklaring skulle kunna vara förekomsten av strukturerad data inom läkemedelsområdet och av en nationell hantering av e-recept. Den nationella användningen av övriga besluts- och kunskapsstöd är däremot begränsad, även om det finns flera exempel på att enskilda landsting eller kliniker utvecklar egna beslutsstöd anpassade till den egna verksamheten.

[3] SOU 2015:32, s. 262.
[4] SOU 2015:32, s. 121 f.

När det gäller ett säkert och ändamålsenligt informationsutbyte i hälso- och sjukvården finns det utmaningar även ur ett organisatoriskt perspektiv. Hälso- och sjukvården bedrivs av 21 självständiga landsting och regioner samt 290 kommuner. Apotekssektorn består i dag av ett 25-tal aktörer som driver cirka 1 300 apotek. Några exakta uppgifter om hur många vårdgivare det finns i dag i Sverige är inte möjligt att få fram. En siffra som har nämnts i olika sammanhang är att det finns omkring 10 000 privata vård- och omsorgsföretag i Sverige.

Alla dessa aktörer har mängder med system (journalsystem, dokumentationssystem, bildhanteringssystem etc.), databaser, moduler, servrar m.m. Varje landsting har hundratals, kanske tusentals, system. Enligt E-hälsokommittén[5] har exempelvis Region Västra Götaland omkring 2 000 system, Stockholms läns landsting cirka 1 300 system och landstinget Dalarna runt 300 olika system. Lägger man till kommuner, privata och idéburna vård- och omsorgsgivare, apotek samt statliga myndigheter som bedriver hälso- och sjukvård är mängden system i landet helt oöverskådlig.

Beträffande system för vårddokumentation, finns det dock inte samma spridning på olika system, enligt den senaste SLIT-rapporten.[6] Det anförs i rapporten att det i dag är ett fåtal system och leverantörer som dominerar marknaden. Fem leverantörer har med sina åtta system 97,6 procent av alla användare. Det framgår vidare att flertalet landsting har standardiserat med ett system och en leverantör för all vårddokumentation inom den egna organisationen, dvs. för sjukhus, psykiatri och primärvård. Starka drivkrafter är enligt SLIT-rapporten visionen om ”en patient – en journal” med gemensam läkemedelslista och gemensam term- och begreppsstruktur. Intern konsolidering med endast en instans (en databas) sägs underlätta och vara ett steg på vägen att nå visionen så att informationen kan bli tillgänglig såväl inom landstinget som över huvudmannagränser.

Landstingen har en särställning som både huvudmän och vårdgivare. Det är landsting och kommun som finansierar vården. De flesta landstingen kräver eller erbjuder att privata vårdgivare som ingår i vårdvalet ska använda samma journalsystem som landstinget.[7]

[5] SOU 2015:32.

[6] SLIT-gruppens (landstingens it-strateger och it-chefer) rapport eHälsa i landstingen 2015 (SLIT-rapporten).

[7] SLIT-rapporten 2015.

Information hanteras inte enbart av och mellan vårdgivare inom samma sjukvårdshuvudman för syftet att ge hälso- och sjukvård i det enskilda fallet. Patientuppgifter används även i uppföljningssyften, kvalitetsregister, forskning, utbildning och till exempel för administration av patienttransporter.

Personuppgifter har också ett kommersiellt värde. Det finns ett stort intresse från olika håll av att få använda vårdinformation som råmaterial i tjänster. Det kan t.ex. bli möjligt genom den planerade tjänsten HälsaFörMig.

HälsaFörMig är ett hälsokonto som eHälsomyndigheten ansvarar för. Tanken med kontot är att enskilda ska få möjlighet att samla all information om sin hälsa på ett och samma ställe. Hälsokontot ska fungera som en tjänst som gör det möjligt för var och en att överblicka sin egen hälsoinformation över tid. Enligt eHälsomyndighetens bedömning är det individen själv som ansvarar för innehållet i HälsaFörMig och får bestämma om någon ska ges behörighet att läsa eller hämta information. eHälsomyndigheten ska vara ansvarig för att informationen hanteras på ett säkert sätt. Myndigheten ska erbjuda tredje part möjlighet att ansluta tillämpningar (appar) och tjänster till hälsokontot, men sedan är det individen som ska välja vilka e-tjänster han eller hon vill använda för att bearbeta och visa upp sin information.

Problembeskrivningar och förslag avseende e-Hälsa i andra utredningar

E-hälsa beskrivs i E-hälsokommitténs betänkande[8] som insatser för att med hjälp av informationssystem och e-tjänster skapa och utveckla en ändamålsenlig och säker informationshantering inom och mellan hälso- och sjukvården och socialtjänsten, till nytta för individer, professioner och beslutsfattare.

Olika aspekter av området e-Hälsa har utretts de senaste åren av Utredningen om rätt information i vård och omsorg[9], E-hälsokommittén och av den nationella samordnare[10] som regeringen utsett för effektivare resursutnyttjande inom hälso- och sjukvården.

[8] SOU 2015:32 s. 72.
[9] SOU 2014:23.
[10] Ett tidsbegränsat och numera avslutat uppdrag som beskrivs i dir. 2013:104.

I april 2014 lämnade Utredningen om rätt information i vård och omsorg sitt slutbetänkande. Utredningen lämnade en rad förslag beträffande elektroniska patientjournaler. Bland annat föreslås att samtliga vårdgivare som finansieras av samma huvudman ska kunna dela uppgifter om en patient med hjälp av direktåtkomst under samma förutsättningar, oavsett om verksamheten drivs i offentlig eller privat regi. Utredningen lämnar även förslag som innebär tydligare krav på informationssystemens utformning. Vidare föreslås att det inte längre ska gå att spärra uppgifter om förskrivna läkemedel och om överkänslighet.

Många menar att utredningens förslag på ett bra sätt väger in behovet av skydd för patienternas personliga integritet, medan t.ex. Justitieombudsmannen, Justitiekanslern, Myndigheten för samhällsskydd och beredskap, Datainspektionen och Sveriges advokatsamfund skarpt kritiserar förslaget för att det inte tillräckligt beaktar den personliga integriteten.

I betänkandet *Effektiv vård*[11] konstateras att informationssystemen i hälso- och sjukvården lider av stora brister. Bland de problem som lyfts fram är brister i design, funktionalitet och överskådlighet liksom brister när det gäller struktur och enhetlighet i termer och begrepp. Vidare finns brister när det gäller systemens möjlighet att kommunicera med varandra över vårdgivargränserna, inom en vårdgivare och till och med för en och samma användare. I betänkandet anförs även att arbetet med att implementera integritetsskydd för patienten (t.ex. åtkomstkontroll) måste bli bättre. Den nationella samordnaren påpekar att även om det pågår många olika utvecklingsinitiativ så saknas det väsentligen någon samordning av arbetet. Trots många års kännedom om problemen har huvudmännen varit oförmögna att agera samlat i investeringar, kravställande, utvecklingsarbete och standardisering m.m.

E-hälsokommittén[12] påtalade i sitt betänkande behoven av en tydligare styrning från nationell nivå för att utveckla interoperabilitet över organisations- och huvudmannagränser. Det finns enligt E-hälsokommittén behov av koordination av insatser som pågår men också av att etablera nya arenor för nationellt arbete, av att enas kring vilka krav på teknik, informationssäkerhet och integritetsskydd som

[11] Slutbetänkande av den nationella samordnaren för effektivare resursutnyttjande inom hälso- och sjukvården, SOU 2016:2, s. 285 ff.
[12] SOU 2015:32.

måste uppnås samt av att någon aktör på nationell nivå har mandat att besluta om sådana krav. Kommitténs uppfattning var att tillämpning av standarder och krav är en nyckelfråga för att åstadkomma denna ökade semantiska och tekniska interoperabilitet och föreslog därför ett statligt ansvar för att besluta om sådana krav.

E-hälsokommitténs betänkande har kritiserats ur ett integritetsperspektiv. Exempelvis anser Datainspektionen och Justitieombudsmannen menade att betänkandet saknar analyser av konsekvenserna för den personliga integriteten.

Vision e-Hälsa 2025

Regeringen och Sveriges kommuner och landsting (SKL) har i mars 2016 beslutat att ställa sig bakom en gemensam vision för e-hälsoarbetet fram till år 2025. Visionen ersätter den tidigare e-Hälsostrategin från 2010 och lyder:

> År 2025 ska Sverige vara bäst i världen på att använda digitaliseringens och e-Hälsans möjligheter i syfte att underlätta för människor att uppnå en god och jämlik hälsa och välfärd samt utveckla och stärka egna resurser för ökad självständighet och delaktighet i samhällslivet.

Arbetet ska drivas utifrån ett antal grundläggande perspektiv och principer som tillgänglighet, användbarhet och digital delaktighet, samt integritetsskydd och informationssäkerhet.

9.3 Behörighetsstyrning, åtkomstkontroll och spärrar och annan hantering av personuppgifter inom en vårdgivares verksamhet

9.3.1 Företeelsen

I det här avsnittet tar vi upp hur uppgifter hanteras när den enskilde är patient och mottagare av hälso- och sjukvård. De företeelser som nämns nedan har valts ut eftersom vi anser dem särskilt beaktansvärda ur ett integritetsskyddsperspektiv. I detta avsnitt är det den digitala hanteringen som görs av personal som är verksam hos en och samma vårdgivare som behandlas. I ett följande avsnitt avhandlas

personalen möjlighet att genom elektronisk direktåtkomst ta del av uppgifter om patienter som vårdats hos andra vårdgivare, så kallad sammanhållen journalföring.

Grundläggande förutsättningar för en ändamålsenlig informationshantering är bland annat att uppgifter finns tillgängliga när de behövs för vården av en patient. En annan förutsättning är att de uppgifter som dokumenteras om patienter förvaras och hanteras på ett sådant sätt att obehöriga inte kan komma åt dem, att uppgifter inte sprids utanför verksamheten, att de informationssystem som används i verksamheten är utformade på ett sådant sätt att integritetsskyddet tillgodoses, att en användares behörighet till uppgifter anpassas och begränsas till de behov som användaren har samt att åtkomsten till uppgifterna loggas och kontrolleras.

Digitalt hanterade uppgifter hos vårdgivarna är ofta åtkomliga och läsbara för en stor grupp anställda hos den aktuella vårdgivaren. Men uppgifter kan göras läsbara även för anställda hos andra vårdgivare på olika håll runtom i landet genom s.k. sammanhållen journalföring.

Det är vårdgivaren som har det yttersta ansvaret för informationssäkerheten i verksamheten. Ansvaret innebär bl.a. att vårdgivaren måste se till att de informationssystem som används i verksamheterna är skyddade mot obehörig åtkomst och att det finns bra system för tilldelning av behörighet och åtkomstkontroll.

När det gäller spärrar framgår det av den så kallade SLIT-rapporten för 2015 att det är ovanligt att patienter begär att få spärra information. Det rör sig om ungefär 122 patienter per landsting och år. Ungefär 10 patienter per år begär att få häva spärren. Det framgår inte av uppgifterna om det är patienter som begärt att få spärra uppgifter inom vårdgivaren eller om det är patienter som inte velat delta i sammanhållen journalföring.

Tidningen Vårdfokus uppmärksammade i april 2013 att det under år 2012 polisanmäldes minst 56 anställda i landsting och regioner för att olovligen ha gått in i patientdatajournaler, vilket innebar en ökning med mer än 100 procent jämfört med år 2010. Enligt tidningen kunde det dock i verkligheten röra sig om ännu fler polisanmälningar, på grund av att det exakta antalet är svårt att få fram eftersom somliga landsting saknar central uppföljning och därmed inte har en samlad bild av intrång som görs i den egna organisationen. Enligt tidningen var det fler än de 56 polisanmälda som hade misstänkts och utretts

internt utan att det blivit någon polisanmälan.[13] Antalet polisanmälda dataintrång kan ställas i relation till att det görs cirka 65 miljoner patientbesök i hälso- och sjukvården per år[14] och att det finns över 200 000 anställda[15] i landstingens hälso- och sjukvård.

9.3.2 Det skyddande regelverket

I patientdatalagen och Socialstyrelsens anslutande föreskrifter (SOSFS 2008:14) stadgas i korthet att vårdgivare måste sörja för bl.a. följande.

Vårdgivaren ska säkerställa att det i verksamhetens ledningssystem för kvalitet och patientsäkerhet finns en dokumenterad informationssäkerhetspolicy. Den ska säkerställa att

1. patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig (tillgänglighet),
2. patientuppgifterna är oförvanskade (riktighet),
3. obehöriga inte ska kunna ta del av patientuppgifterna (sekretess), och
4. det i sådana informationssystem som är helt eller delvis automatiserade är möjligt att i efterhand entydigt kunna härleda åtgärder till en identifierad användare (spårbarhet).

Det är av integritetsskäl viktigt att inte andra personuppgifter behandlas inom hälso- och sjukvården än vad som är befogat utifrån verksamhetens behov och krav. En vårdgivare eller en huvudman får därför endast behandla sådana uppgifter som behövs för de ändamål som i lagen räknas upp som tillåtna. En ändamålsbestämmelse i patientdatalagen styr därmed över vilka personuppgifter som får samlas in och fortsättningsvis behandlas i verksamheten.

Det måste vidare finnas rutiner som säkerställer att individuell behörighetstilldelning görs. Det innebär enligt Socialstyrelsens handbok till föreskrifterna att endast personliga inloggningar är tillåtna och att inga så kallade gruppkonton får förekomma. Använ-

[13] Helena Mirsch, *Allt fler polisanmäls för dataintrång*, publicerad den 3 april 2013 på www.vardfokus.se
[14] SKL, Statistik om hälso- och sjukvård samt regional utveckling 2013.
[15] SKL, Statistik anställda i landstingen 2014.

darnas behörighet i vårdgivarens informationssystem måste vara anpassad till deras arbetsuppgifter. Vårdgivaren ansvarar också för att användarna tilldelas rätt behörighet, det vill säga tillräckliga behörigheter för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt men samtidigt inte mer omfattande än vad som är nödvändigt.

Vidare måste det finnas rutiner som säkerställer att åtkomstkontroll genomförs. Det är enbart tillåtet att ta del av dokumenterade uppgifter om en patient om man deltar i vården av en patient eller om man av andra skäl behöver uppgifterna för sitt arbete åt vårdgivaren. Även om personalen kan få fram uppgifterna får de inte ta del av några patientuppgifter som de inte behöver för att sköta sitt arbete. För att vårdgivaren ska kunna kontrollera att behörigheterna används på ett korrekt sätt måste denne dokumentera (logga) åtkomsten till de uppgifter som har använts.

Vidare ska systemet kräva aktiva val för åtkomst till patientuppgifter från andra enheter. Enligt förarbetena[16] till patientdatalagen bör uppgifter lagras i olika skikt så att mer känsliga uppgifter kräver aktiva val eller inte är lika lätta att nå som mindre känsliga uppgifter. Enligt Socialstyrelsens handbok till föreskrifterna menas med aktiva val att en behörig användare tar ställning till om han eller hon har rätt att ta del av ytterligare uppgifter.

Vidare har en patient rätt att ”spärra uppgifter” vilket innebär att patienten motsätter sig att uppgifter om honom eller henne är elektroniskt tillgängliga för andra vårdenheter eller vårdprocesser än den som patienten varit i kontakt med. Det betyder att hälso- och sjukvårdspersonal från andra enheter inom vårdgivarens verksamhet inte får ta del av uppgifterna, om det inte är frågan om så kallad nödåtkomst, se 4 kap. 5 § patientdatalagen.

9.3.3 Iakttagelser från tillsynen

När det gäller behörighetsstyrning och åtkomstkontroll i elektroniska journaler, har Datainspektionen riktat kritik mot olika vårdgivare i ett antal ärenden på senare år.

I maj 2014 publicerade Datainspektionen resultaten av en granskning av hälso- och sjukvården i 18 kommuner med särskild inriktning på vilka åtgärder som tas för att hindra obefogad och okontrollerad

[16] Regeringens proposition *Patientdatalag m.m.*, prop. 2007/08:126 s. 149.

spridning av patientuppgifter. Granskningen visade på brister hos samtliga kommuner. Förekommande brister var bl.a. att det saknades dokumenterade behovs- och riskanalyser och att det inte gjordes verkningsfulla loggkontroller. Vidare förekom brister i informationen till de anställda om att loggning och logguppföljning görs samt om vilka villkor som gäller för anställdas åtkomst till patientuppgifter.

I juni 2013 redovisade Datainspektionen resultaten av en nationell kontroll av vårdgivare om hur dessa kan spärra känsliga patientuppgifter när en patient begär det. Granskningen visade att många vårdgivare hade börjat satsa ordentligt på att införa de möjligheter till spärrar som måste finnas enligt patientdatalagen. Vissa av vårdgivarna har således kommit en bra bit på väg och vissa var enligt Datainspektionen i praktiken framme vid målet. Det fanns dock några vårdgivare som inte hade kommit lika långt när det gäller införandet av tekniska funktioner för spärrar i it-systemen.

I april 2012 kritiserade Datainspektionen ett av landets största sjukhus för att dess it-system gjorde det omöjligt att kontrollera om personal missbrukar sin möjlighet att läsa patientjournaler.

I augusti 2013 fann Datainspektionen brister i rutinerna för behörighetsstyrning och åtkomstkontroll hos ett annat av landets största sjukhus. Sjukhuset förelades att genomföra en behovs- och riskanalys för sitt journalsystem för att kunna arbeta effektivt med behörighetsstyrning och åtkomstkontroll.

9.3.4 Risker för den personliga integriteten

Regelverket beträffande behörighetsstyrning, åtkomstkontroll och spärrhantering ska skydda patienternas uppgifter och ge patienterna ett viss mått av inflytande över när uppgifterna får behandlas. För att uppfylla patientdatalagens krav kan det röra sig om såväl tekniska som organisatoriska eller administrativa åtgärder. Behörighetsstyrning och logguppföljning är skyldigheter som åligger vårdgivarna, och påverkas inte av patienternas inställning.

Om vårdpersonalen får veta saker om patienten som de inte behöver veta och som patienten inte vill att de ska få reda på, t.ex. att en ortopedspecialist får veta att och varför patienten vårdats vid en annan klinik hos samma vårdgivare, kan detta väcka obehag hos patenten, och påverka hur hon eller han upplever mötet med vården.

Det kan också innebära att patienten inte berättar lika öppet om sina besvär nästa gång hon eller han uppsöker vården, vilket i sin tur kan medföra en sämre vård.

Det finns vissa risker för ren nyfikenhetsläsning, t.ex. att en granne, släkting, bekant eller kollega inom vården läser patientuppgifter för att hon eller han är nyfiken på patienten. Ju mer information varje anställd kan ta del av, desto större är den potentiella skadan vid nyfikenhetsläsning och eventuell senare spridning genom skvaller. Om patienten dessutom råkar vara känd på orten, ökar risken för nyfikenhetsläsning av en större grupp vårdpersonal. Nyfikenhetsläsning kan naturligtvis förekomma även i samband med hantering av patientjournal på papper. Vid sådan hantering är det dock svårt att i efterhand kontrollera vilka som tagit del av informationen.

Slutligen finns en risk för dataläckage, genom medvetna attacker, vårdslöshet eller bristande kunskaper hos vårdgivarens anställda.

Det bör också framhållas att uppgifter om patienter hos vårdgivarna kan vara av intresse inte bara för hälso- och sjukvårdspersonal – den kan också vara intressant för utomstående som försäkringsbolag och polismyndigheter, som under vissa förutsättningar kan få ta del av dessa.

När det gäller kunskap om patientdatalagen bland landstingets personal framgår det av den senaste SLIT-rapporten att situationen har blivit bättre genom att de flesta nu har genomfört utbildningar. Det finns dock fortfarande ett behov av utbildning i några landsting. När det gäller tillämpningen av patientdatalagen framgår det av SLIT-rapporten 2015 att bara två landsting har anpassat systemen så att de klarar de krav som lagen ställer på dem. Det bedömdes att nio landsting kommer att vara klara 2016, medan övriga landsting inte räknar med att vara klara förrän 2017 eller senare. Alltså nästan tio år efter att patientdatalagen infördes.

9.4 Sammanhållen journalföring

9.4.1 Företeelsen

I och med patientdatalagens ikraftträdande blev det lagligen möjligt för vårdgivare att låta andra vårdgivare ta del av verksamhetens patientuppgifter genom direktåtkomst. Stödet för detta finns i 6 kap.

patientdatalagen. Det innebär att patientens uppgifter får göras tillgängliga, inte bara inom den vårdgivare där uppgifterna har tillkommit, utan också under vissa förutsättningar till andra vårdgivare som ingår i ett sådant samarbete och som behöver uppgifterna i vården av patienten.

Enligt SLIT-rapporten 2015 kommer landstingen i första hand att använda denna möjlighet i samverkan med de privata vårdgivarna inom vårdvalet, i andra hand med kommuner och andra landsting. Några landsting kommer också att ha sammanhållen journalföring med privata vårdgivare utan vårdavtal.

9.4.2 Det skyddande regelverket

I 6 kap. patientdatalagen finns bestämmelser om att patienterna ska få information i förväg innan deras uppgifter får göras tillgängliga i ett system för sammanhållen journalföring. De ska även ges möjlighet stå utanför den sammanhållna journalföringen (få s.k. spärr). Användargränssnitten i system för sammanhållen journalföring får initialt bara visa att det finns uppgifter om patienten att läsa i systemet. Andra vårdgivare ska kunna ta del av denna uppgift utan att ta del av uppgift om vilken vårdgivare som har gjort uppgiften tillgänglig. För att den andra vårdgivaren (än den som skrivit in journaluppgifterna) ska få ta del av uppgifterna krävs att denne har en aktuell patientrelation med den enskilde och att uppgifterna i fråga kan antas ha betydelse för den vård som ska ges. Innan uppgifterna används i verksamheten ska den andra vårdgivaren dessutom inhämta patientens samtycke till detta.

9.4.3 Iakttagelser från tillsynen

Även när det gäller sammanhållen journalföring, har Datainspektionen riktat kritik mot olika vårdgivare i ett antal ärenden på senare år.

I februari 2011 kritiserade Datainspektionen tre vårdgivare för att de använde sig av ett system för sammanhållen journalföring där det inte gick att spärra vissa patientuppgifter från att lämnas ut. Datainspektionen var också kritisk till att personalen hos de granskade vårdgivarna i systemet för sammanhållen journalföring hade för omfattande behörigheter och att åtkomstkontrollen var bristfällig.

I januari 2011 kritiserade Datainspektionen Karolinska universitetssjukhuset för brister i informationen till patienterna om sammanhållen journalföring. I april samma år hotade Datainspektionen med att förelägga Karolinska universitetssjukhuset att upphöra med att lämna ut uppgifter inom sammanhållen journalföring, om inte sjukhuset förbättrade informationen till sina patienter om vad den så kallade sammanhållna journalföringen innebär. Patienterna skulle även informeras om att de kan begära att uppgifter spärras.

I juni 2012 konstaterade Datainspektionen efter en tillsyn av samtliga landsting samt fem privata vårdgivare att ingen av de granskade vårdgivarna helt uppfyllde patientdatalagens krav beträffande patienternas rätt att få sina uppgifter i journalerna spärrade.

I juni 2013 redovisade Datainspektionen resultaten av en nationell kontroll av vårdgivare och hur dessa kan spärra känsliga patientuppgifter när en patient begär det. Kontrollen omfattade även spärrhanteringen i system för sammanhållen journalföring. Granskningen visade att många vårdgivare hade börjat satsa ordentligt på att införa de möjligheter till spärrar som måste finnas enligt patientdatalagen. Vissa av vårdgivarna har således kommit en bra bit på väg och vissa var enligt Datainspektionen i praktiken framme vid målet. Det fanns dock några vårdgivare som inte hade kommit lika långt när det gäller införandet av tekniska funktioner för spärrar i it-systemen.

9.4.4 Risker för den personliga integriteten

Sammanhållen journalföring kan ge ökad vårdkvalitet genom en helhetsbild av patientens tidigare diagnoser, provresultat och medicinering vilket gör det lättare att ställa rätt diagnos och ge rätt behandling i tid. Den sammanhållna journalföringen ger också ökad patientsäkerhet genom att ge rätt beslutsunderlag som minskar risken för felbehandlingar eller felmedicinering. Denna form av informationsutbyte är av särskild nytta i samband vård av äldre som bor på särskilda boenden i kommunerna. För att kunna ge säkra insatser för denna patientgrupp behöver den kommunala och landstingskommunala hälso- och sjukvården samarbeta. Sammanhållen journalföring kan också bidra till ökad effektivitet genom att delad information minskar tidsspillan och kostsamt dubbelarbete.

En förutsättning för ändamålsenligt informationsutbyte mellan olika vårdgivare är att det finns en fungerande infrastruktur. E-hälsokommittén[17] föreslog i sitt betänkande att staten bör ges en samordnande roll. Staten bör enligt E-hälsokommittén ställa krav på en grundläggande interoperabilitet så att it-stöd i vård och omsorg kan kommunicera med varandra på ett bättre sätt. Gemensamma standarder, gränssnitt, funktionskrav och informationssäkerhetskrav m.m. skulle öka förutsättningarna för en utveckling av den sammanhållna journalföringen.

Många vårdgivare arbetar med att införa gemensamma tjänster över vårdgivar- och organisationsgränserna för system för sammanhållen journalföring, vilka möjliggör och förbättrar exempelvis funktioner för spärrhantering, behörighetsstyrning och åtkomstkontroll. Ett exempel på detta är Ineras s.k. säkerhetstjänster.

När det gäller skyldigheten att informera patienterna om den sammanhållna journalföringen, finns det tecken på att Datainspektionens tillsynsinsatser haft viss effekt. I juni 2011 ansåg Datainspektionen efter en tillsyn att Karolinska universitetssjukhusets hade förbättrat sin information till patienterna så pass att Datainspektionen inte längre krävde att sjukhuset skulle sluta lämna ut patientuppgifter till andra vårdgivare.

Men det finns fortfarande brister hos stora vårdgivare när det gäller behörighetsstyrning och åtkomstkontroller även i system för sammanhållen journalföring.

Datainspektionens tillsynsärenden visar också att det fortfarande förekommer brister hos flera vårdgivare när det gäller möjligheten att spärra uppgifter.

När det gäller riskerna med system för sammanhållen journalföring anser kommittén att dessa i stort sett är desamma som i samband med den digitala hanteringen inom en vårdgivare, med det betydande tillägget att sammanhållen journalföring möjliggör åtkomst till fler patienters uppgifter för långt fler användare. Det betyder att frågor om behörighetsstyrning, åtkomstkontroll och spärrar är ännu viktigare när det gäller sammanhållen journalföring. Därtill kommer att informationen till patienterna är av särskilt betydelse, eftersom det finns en rätt för patienterna att stå utanför den sammanhållna journalföringen (dvs. en rätt att få uppgifterna spärrade).

[17] SOU 2015:32.

9.5 Kvalitetsregister

9.5.1 Företeelsen

Kvalitetsregister är en särskild kategori uppgiftssamlingar som finns inom hälso- och sjukvården, främst inom vissa medicinska specialiteter. De har oftast byggts upp genom frivilliga initiativ av olika specialistföreningar för att användas som stöd för kvalitetsutveckling i det kliniska arbetet. Gemensamt för kvalitetsregistren är att inrapporteringen är ett frivilligt åtagande från vårdgivarnas sida. De äldsta registren som fortfarande är i drift startades inom ortopedin redan på 1970-talet. Från 1990-talet och framåt har etableringen av nationella kvalitetsregister ökat väsentligt.[18]

Med ett kvalitetsregister avses, enligt 7 kap. 1 § patientdatalagen en automatiserad och strukturerad samling av personuppgifter som inrättats särskilt för ändamålet att systematiskt och fortlöpande utveckla och säkra vårdens kvalitet. Kvalitetsregistren ska möjliggöra jämförelse inom hälso- och sjukvården på nationell eller regional nivå. Med ett nationellt eller regionalt kvalitetsregister avses ett kvalitetsregister i vilket personuppgifter samlas in från flera olika vårdgivare.

I dag används omkring 100 nationella kvalitetsregister för att säkra och utveckla kvaliteten i hälso- och sjukvården. I ett nationellt eller regionalt kvalitetsregister samlas personuppgifter från kommunal hälso- och sjukvård, sjukhus, vårdcentraler m.fl. för att möjliggöra kvalitetssäkring och jämförelser inom hälso- och sjukvården på nationell eller regional nivå. Kvalitetsregistren används i dag både för systematisk uppföljning och jämförelse på nationell nivå, men även på ett mer lokalt plan där registrerande enheter med allt tätare intervall följer sina resultat och lägger dem till grund för ett verksamhetsnära förbättringsarbete.[19]

Kvalitetsregister har kommit att bli en av flera nödvändiga förutsättningar för att utveckla hälso- och sjukvården. Utvecklingen går mot att verksamhetens inrapporterade uppgifter och resultat återförs mer kontinuerligt än tidigare och kan därmed i större grad ligga till grund för en lokal och verksamhetsnära förbättring av resultatet för de enskilda patienterna.

[18] Prop. 2007/08:126 s. 176.
[19] SOU 2014:23, s. 494.

Det medför att patienter som i dag deltar i kvalitetsregister kan vara med och dra nytta av sin medverkan i registret. I sådana register där individen följs upp och uppgifter registreras kontinuerligt och över längre tid finns tydliga exempel på nyttan, inte endast för framtida patienter utan även för patienten själv.

Några exempel på sådana register som kan nämnas är register över kroniska sjukdomar som t.ex. reumatisk sjukdom och diabetes, men även register som Senior Alert och BPSD som riktar sig till individer över en viss ålder eller med en viss beteendemässig störning. I sammanhanget kan även nämnas registret InfCare HIV som sedan det infördes för cirka 10 år sedan anses ha varit en stark bidragande faktor till att HIV-patienter som är under behandling i dag i stor utsträckning kan känna sig friska och leva ett normallångt liv med i princip obefintlig risk att smitta andra. Förbättringsarbetet genom InfCare HIV har i olika sammanhang lyfts upp som ett exempel på när insamlandet av uppgifter blir en förutsättning för att kunna skapa bättre resultat och högre livskvalitet för en hel patientgrupp.[20]

När det fortsättningsvis i detta betänkande talas om kvalitetsregister, avses härmed nationella och regionala kvalitetsregister som förs i enlighet med 7 kap. patientdatalagen.

9.5.2 Det skyddande regelverket

Behandlingen av patienters uppgifter i regionala eller nationella kvalitetsregister ska enligt 7 kap. patientdatalagen bygga på ett opt-out-förfarande. Således krävs inte patientens samtycke för behandling av uppgifterna i registret. Patienten har däremot rätt att när som helst få uppgifter om sig själv utplånade ur registret och motsätta sig framtida registrering i det aktuella kvalitetsregistret.

Dessutom har den ansvariga vårdgivaren en skyldighet att innan uppgifterna behandlas i kvalitetsregistret informera patienterna om att hennes eller hans uppgifter kommer att behandlas i registret, och om att det finns en rätt att motsätta sig att uppgifterna behandlas.

Vårdgivaren får behandla personuppgifter i ett nationellt eller regionalt kvalitetsregister även om den enskilde inte endast tillfälligt saknar förmåga att ta ställning till personuppgiftsbehandlingen. Villkoren för sådan personuppgiftsbehandling är att den enskildes in-

[20] SOU 2014:23,s. 495.

ställning till den så långt möjligt har klarlagts och att det inte finns anledning att anta att han eller hon skulle ha motsatt sig personuppgiftsbehandlingen.

9.5.3 Iakttagelser från tillsyn och myndighetsanalyser

Vid Datainspektionens omfattande tillsyn över nationella kvalitetsregister år 2010 framkom stora och systematiska brister i regelefterlevnaden. De konstaterade bristerna rörde ofullständig information till patienterna, felaktig användning av uppgifterna, utebliven gallring av uppgifter och otydlig organisation där vårdgivarna inte visste vem som ansvarade för vad. Datainspektionen konstaterade att vårdgivare i stor utsträckning lämnade ut uppgifter till kvalitetsregister utan att veta vem som tar emot patienternas uppgifter och ansvarar för den fortsatta hanteringen, vilket strider både mot bestämmelser om sekretess och grundläggande krav i personuppgiftslagen. Vidare förelades de ansvariga vårdgivarna att vidta tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifterna i systemet vid överföring över öppet nät såsom internet eller Sjunet.[21]

En faktor som kan minska de ansvarigas benägenhet att följa regelverket, är förekomsten av ekonomisk ersättning för varje patient som registreras i ett kvalitetsregister. Ett exempel på detta är en kommun som fick beskedet från Datainspektionen att registrering av personer som varaktigt saknade beslutsförmåga inte var tillåten i kvalitetsregister, men som därefter ändå fortsatte registreringen.[22] Det aktuella registret omfattades av den s.k. ”Äldresatsningen” som innebar att kommuner och landsting som valde att rapportera till vissa register ersattes ekonomiskt.

Vidare har, sedan Datainspektionens tillsyn, staten och Sveriges Kommuner och Landsting (SKL) ingått en överenskommelse om en satsning på de nationella kvalitetsregistren. Satsningen innebär ett ökat finansiellt stöd till registerverksamheten under perioden 2012–2016 och omfattar sammanlagt drygt en och en halv miljard kronor.

[21] Datainspektionens beslut den 11 oktober 2010 i ärenden med dnr 1604-2009, 1605-2009, 1606-2009 och 1725-2009.

[22] Datainspektionens beslut den 15 mars 2013, dnr 1049-2012.

Tre stödfunktioner är knutna till satsningen: kansliet för Nationella Kvalitetsregister, sex regionala registercentrum och Registerservice på Socialstyrelsen.[23]

I en nyligen genomförd granskning av kvalitetsregistren, uttalar Myndigheten för vårdanalys kritik mot systemet med tillfälliga prestationsmedel i syftet att öka inrapporteringen till kvalitetsregistren. Myndigheten tror att det i vissa fall till och med kan vara demoraliserande och långsiktigt skadligt för registren att ekonomisk ersättning ges till landstingen och kommunerna då verksamheterna – vilka vanligen inte får del av ersättningarna – ska rapportera in i register även om de inte uppfattar registren som användbara.[24]

När det gällde den gemensamma satsningen anförde myndigheten bl.a. att

> Satsningen har inneburit ett ökat stöd till registren i juridiska frågor både från de regionala registercentrumen och från kansliet för Nationella Kvalitetsregister. Trots detta anger bara nio procent av de nationella kvalitetsregistren att de kunnat genomföra viktiga förändringar inom juridikområdet sedan satsningen infördes. Flera registerhållare vittnar om att de hittills haft lite kontakt med personuppgiftsombud eller annan juridisk kompetens. Samtidigt anger 47 procent att de vill se ett ökat juridiskt stöd. Resultaten visar exempelvis att kvalitetsregistren delvis gör olika tolkningar och tillämpningar av hur patienterna ska informeras om registret och hur samtycke ska inhämtas. Ett annat område som registren skulle behöva utökat stöd inom rör hur beslutsstöd kan hanteras i relation till gällande lagstiftning. Patientföreträdares inställning till information och sekretess skiljer sig åt sinsemellan men gemensamt är att flera ser förbättringspotential på området.

Beträffande it-stöden för kvalitetsregistren sägs i rapporten att vissa framsteg har gjorts, men att mer stöd är starkt prioriterat från registrens sida och att behovet av samordning är fortsatt stort.

Även om direkta frågor om informationssäkerhet inte har ställts i Myndighetens för vårdanalys utvärdering, ger den generella bristen på it-samordning anledning att anta att det fortfarande kan finnas en del brister när det gäller informationssäkerheten hos registren.

---

[23] *Registrera flera eller analysera mera? Delutvärdering av satsningen på nationella kvalitetsregister*, Rapport 2014:9 från Myndigheten för vårdanalys, s. 7, 12, 52.

[24] *Registrera flera eller analysera mera? Delutvärdering av satsningen på nationella kvalitetsregister*, Rapport 2014:9 från Myndigheten för vårdanalys.

Som en följd av Datainspektionens tillsynsinsats år 2010 har vårdgivare, företrädare för nationella kvalitetsregister, registercentra och Sveriges kommuner och landsting drivit ett arbete för att ta fram korrekt och fullständig patientinformation.[25]

9.5.4 Risker för den personliga integriteten

En bedömning av läget för kvalitetsregistren år 2014 gjordes av Utredningen om rätt information i vård och omsorg. Det var utredningens uppfattning att medvetenheten om regelverkets krav och vilka åtgärder som är nödvändiga att vidta har ökat bland vårdgivare. Utredningen hade även i samband med konferenser och i möten med s.k. registerhållare för nationella kvalitetsregister fått information som visat på att frågorna prioriterats och att förståelsen för patientinformationen som en grundläggande och integritetsskyddande rättighet är stor.[26]

Staten, kommunerna och landstingen har under senare år satsat ansenliga resurser på att utveckla kvalitetsregistren och öka registreringsgraden, varför dessa register kan förväntas både öka i omfång (fler uppgifter om fler patienter) och även användas mer.

Kvalitetsregister kan, som framgår ovan, både vara av stor nytta för den enskilde patienten och bidra till att förbättra kunskapsläget inom hela hälso- och sjukvården. Men i regel rör det sig om mycket känsliga uppgifter om patienterna. Registren innehåller dessutom uppgifter om en stor del av landets befolkning. Läckor eller felaktig användning av registren kan få betydande effekter på de enskilda. Här kan nämnas att bakgrunden till Datainspektionens breda tillsyn av kvalitetsregistren år 2010 var just felaktig användning. Uppgifter från ett kvalitetsregister hade använts för att skicka ut s.k. ”tiggarbrev” till patienter där patienternas sjukdomar åberopades. Förfarandet ledde till flera klagomål till Datainspektionen som beslutade att genomföra en bred tillsynsinsats. Som nämnts ovan resulterade granskningen i omfattande kritik från Datainspektionen och beslut om att de ansvariga behövde vidta åtgärder på en rad olika områden för att uppfylla patientdatalagens krav.

[25] SOU 2014:23, s. 509 ff.
[26] SOU 2014:23.

9.6 Välfärdsteknik inom socialtjänsten

Socialtjänstens verksamhet ska präglas av respekt för den enskildes självbestämmande, integritet, trygghet och värdighet. Den som tar emot vård- och omsorgsinsatser ska ha möjlighet att vara delaktig i och ha inflytande över beslut och planering av den egna vården och omsorgen samt hur vården och omsorgen utförs enligt socialtjänstlagen. Användning av välfärdteknik[27] måste utgå från respekt för individers önskemål och behov.

Välfärdsteknik kan bland annat handla om användning av olika digitala tjänster i form av trygghetslarm, tele- och videokommunikation, sensorer i hemmet, kognitiva hjälpmedel, ett mobilt arbetssätt och e-tjänster för trygghet, service och delaktighet.

Välfärdsteknik kan bidra till att äldre personer och personer med funktionsnedsättning kan välja att bo kvar hemma och få den omsorg man behöver i hemmet. Sådana tjänster kan också bidra till ett fortsatt aktivt och socialt liv.

9.6.1 Används välfärdsteknik i dag?

Sverige ligger enligt uppgifter från Myndigheten för delaktighet längst fram i Europa med teknikskiftet till digitala trygghetslarm. Ett fåtal svenska kommuner ligger mycket bra till vad det gäller införandet av digitala tjänster inom socialtjänsten och hemsjukvården vid en europeisk jämförelse. Vissa svenska kommuner, som Västerås stad, ligger före vad det gäller socialtjänsten, men vad gäller ett brett införande i landet ligger exempelvis Skottland före Sverige.[28]

9.6.2 Företeelsen

Många äldre har någon form av fysisk eller psykisk funktionsnedsättning som innebär svårigheter i det vardagliga livet och ett ökat behov av vård. Ett mål med äldrepolitiken och kommunernas omsorg om äldre har länge varit att man ska kunna leva och bo själv-

[27] Välfärdsteknik är enligt Socialstyrelsens termbank digital teknik som syftar till att bibehålla eller öka trygghet, aktivitet, delaktighet eller självständighet för en person som har eller löper förhöjd risk att få en funktionsnedsättning. Välfärdsteknologi definieras i termbanken som kunskapen om välfärdsteknik.

[28] Myndighetens för delaktighet Delrapport 2014, *Digitala tjänster*.

ständigt och under trygga förhållanden.[29] Ofta innebär detta att den äldre bor kvar i sitt hem där han eller hon får stöd och vård i form av hemtjänst när hälsan sviktar. Den demografiska utvecklingen med ett ökat antal äldre har aktualiserat diskussioner och utredningar om hur resursbesparingar och effektivisering av hälso- och sjukvården samt omsorgen om äldre kan genomföras.

Övervakning med hjälp av robotar, videokameror och GPS-sändare används i huvudsak som ett alternativ eller ett komplement till vård- och omsorgspersonalens fysiska tillsyn av den äldre personen i hans eller hennes hem. Det kan finnas flera syften med att använda övervakning. Ett syfte kan vara att stärka den enskildes självbestämmande och integritet genom att han eller hon i större utsträckning själv kan bestämma över sin vardag. Andra syften kan vara att förbättra säkerheten för den enskilde eller att spara in på personalresurser.[30] I flera kommuner har videoövervakning införts som ett alternativ till nattliga hembesök av hemtjänsten. Hemtjänstpersonal kan via en kamera i den äldre personens sovrum under natten kontrollera om personen ser ut att må bra. I Västerås kommun ringer hemtjänstpersonal upp kameran från en dator och kan se en svartvit rörlig bild av det som finns framför den, vanligtvis sängen och delar av sovrummet. Ingen röstkommunikation är möjlig och den enskilde kan inte se personalen. Endast behöriga användare ska kunna komma åt kameran, ingen inspelning görs och insyn ges endast vid i förväg överenskomna tillfällen.[31]

En annan typ av övervakning är när den äldre bär en GPS-sändare på sig så att det går att kontrollera var han eller hon befinner sig. Sådan övervakning görs genom s.k. mobila trygghetslarm med inbyggd GPS. Ett trygghetslarm går ut på att person som bär det på sig kan larma anhöriga, vårdpersonal eller en larmcentral. Om larmet även har en inbyggd GPS-sändare kan de som har fått behörighet även kontrollera var personen befinner sig. Ett syfte med GPS-sändaren kan vara att hitta en äldre person som gått vilse. Det är således oftast personer med demenssjukdom som är av intresse att övervaka på det här sättet.

[29] Regeringens skrivelse 2013/14:57 *Ett värdigt liv* – äldrepolitisk *översikt 2006–2014* samt socialtjänstlagen (2001:453).

[30] *Robotar och övervakning i vården av äldre – etiska aspekter*, rapport av Statens medicinsk-etiska råd Stockholm 2014, s. 27 ff.

[31] www.viktigvasteras.se/ehemtjanst/tekniska-losningar/, hämtat den 26 april 2016.

9.6.3 Det skyddande regelverket

Kommunernas ansvar för socialtjänsten och dess verksamhet, vilken bl.a. omfattar omsorg till äldre genom hemtjänst och särskilda boenden, regleras i socialtjänstlagen.

Verksamheter som styrs av socialtjänstlagen eller lagen om stöd och service till vissa funktionshindrade ska bygga på respekt för den enskildes självbestämmande och integritet. Detta innebär att frivillighet för den enskilde är utgångspunkten för alla insatser.

Båda dessa lagar bygger således på frivillighet och förutsätter samtycke från den enskilde. Det finns dock inga regler innehållande uttryckliga krav på samtycke eller krav gällande hur ett samtycke ska lämnas. Det torde därför enligt Utredningen om beslutsoförmögnas ställning i vård, omsorg och forskning[32] finnas ett visst utrymme för att använda olika former av s.k. presumerade, och kanske i vissa fall hypotetiska, samtycken men det är oklart i vilka situationer och under vilka förutsättningar.

När det gäller kameraövervakning finns särskilda bestämmelser i kameraövervakningslagen (2013:460). Inom ramen för sitt tillämpningsområde gäller alltså den lagen i stället för personuppgiftslagen. Kameraövervakningslagens syfte är att tillgodose behovet av kameraövervakning för berättigade ändamål, samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten. I kameraövervakningsförordningen (2013:463) finns kompletterande regler om bl.a. tillsyn.

Kameraövervakningslagen gäller endast kameraövervakning med TV-kameror, eller därmed jämförbar utrustning, som är uppsatta så att de, utan att manövreras på platsen, kan användas för personövervakning samt behandling av bild- och ljudmaterial som tagits upp vid sådan övervakning. Från lagens tillämpningsområde är dessutom undantaget kameraövervakning av plats dit allmänheten inte har tillträde, om övervakningen bedrivs av en fysisk person som ett led i verksamhet av rent privat natur.

Huvudregeln enligt kameraövervakningslagen är att personen som ska övervakas har samtyckt till övervakningen (22 §). Ett samtycke ska vara en frivillig, särskild och otvetydig viljeyttring från den

[32] Utredningens om beslutsoförmögnas ställning i vård, omsorg och forskning betänkande *Stöd och hjälp till vuxna vid ställningstaganden till vård, omsorg och forskning*, SOU 2015:80, s. 430.

övervakades sida. Det behöver inte vara skriftligt men förutsätter att den som ska övervakas fått information och fullt ut förstår innebörden av samtycket. Att ett samtycke ska vara frivilligt innebär att den som ska samtycka upplever att han eller hon har ett fritt val.

9.6.4 Smers rapport om robotar och övervakning i vården av äldre

Statens medicinsk-etiska råd (Smer) har på eget initiativ tagit fram en rapport[33] om etiska aspekter på robotar och övervakning i vården av äldre. Målet med rapporten är att stimulera till samhällelig diskussion och att utgöra ett stöd inför beslut om användande av robotar och övervakning inom hälso- och sjukvården samt socialtjänstens omsorg om äldre personer.

Rådet anför i rapporten att innan övervakningsåtgärder införs i hälso- och sjukvården samt socialtjänsten, måste en bedömning göras av vilka konsekvenser övervakningen kan få för etiska värden. Det är därför enligt rådet avgörande att noggranna bedömningar görs i varje enskilt fall så att individens rätt till självbestämmande, integritet och lika vård på lika villkor respekteras samt att krav på god vård och omsorg av god kvalitet uppfylls.

En sådan bedömning måste göras innan övervakning börjar användas. I verksamheterna bör det finnas en person som är ansvarig för detta.

I och med att tillsynen som kan genomföras med hjälp av enbart en kamera är begränsad, ser rådet en risk med att använda kameran som ersättning för personliga besök om inte övervakningen kompletteras med annan tillsyn eller ytterligare tekniska lösningar.

Rådet betonar särskilt att det är viktigt att balans uppnås mellan nyttan av övervakningen och det intrång i den enskildes integritet som övervakningen innebär. Åtgärder bör därför vidtas så att integritetsintrånget blir så begränsat som möjligt.

[33] *Robotar och övervakning i vården av äldre – etiska aspekter*, rapport av Statens medicinsk-etiska råd Stockholm 2014.

9.6.5 Risker för den personliga integriteten

De personuppgifter som hanteras inom socialtjänsten är i allmänhet av mer integritetskänslig karaktär än uppgifter som hanteras i andra sammanhang. Socialtjänsten hanterar många uppgifter om enskildas privata förhållanden, som t.ex. om hälsa och om sociala och ekonomiska förhållanden. Av hänsyn till behovet av skydd för den personliga integriteten är det därför nödvändigt att uppgifter om enskilda hanteras på ett säkert och ändamålsenligt sätt. Det handlar även om att inte äventyra enskildas förtroende för socialtjänsten.

Det är landets kommuner som ansvarar för socialtjänsten. Detta ansvar kan kommunen antingen ta genom att själv utföra olika tjänster eller genom att sluta avtal med annan om att utföra kommunens uppgifter. Kommunernas möjligheter att genom upphandling eller införande av valfrihetssystem överlåta utförandet av socialtjänst till privata aktörer har gjort att mångfalden av utförare i dag är betydligt större än vad det har varit tidigare.

De känsliga uppgifter som hanteras inom socialtjänsten hanteras således inte bara av kommunen utan också av olika privata utförare. Det faktum att det inte bara är offentliga organ som hanterar de känsliga uppgifter som finns i socialtjänstens verksamhet ställer särskilda krav på säkerhet.

Olika insatser inom socialtjänsten liksom den informationshantering som hör ihop med insatserna förutsätter att den enskilde själv kan ta ställning och ge uttryck för sin vilja i olika avseenden.

Socialtjänsten möter dock ofta personer som tillfälligt eller mer varaktigt saknar möjlighet att ge uttryck för sin inställning och vilja att exempelvis få en viss vård- och behandlingsinsats. En sådan person har ofta även nedsatt förmåga att ta emot information och lämna samtycke till den informationshantering som vård- och behandlingsinsatserna kräver.

Många av de tjänster som personer med avsaknad av beslutsförmåga har behov av kan inte i dag ges med uttryckligt och tydligt lagstöd i lagstiftningen på omsorgens område. Lagstiftningen på omsorgens område tillhandahåller alltså inte verktyg för att tillgodose att dessa personer ges insatser på lika villkor som andra.[34] Utredningen om hjälp vid ställningstagande till vård, omsorg och forsk-

[34] SOU 2015:80, s. 436.

ning[35] har lämnat förslag till lagstiftning som gör det möjligt att utse företrädare för personer som inte har förmåga att i olika situationer själva ta ställning i frågor som gäller deras hälso- och sjukvård och omsorg.

Användning av olika digitala och tekniska lösningar i socialtjänsten såsom kameraövervakning, GPS-sändare och sensorer m.m. innefattar hantering av mycket nära och känsliga uppgifter om enskilda personer med stort hjälpbehov. Socialtjänsten berör stora delar av befolkningen. Äldre personer behöver ofta någon form av hjälp och stöd från socialtjänsten. Det finns oklarheter i lagstiftningen om på vilket sätt personer med nedsatt beslutsförmåga kan erbjudas tjänster med hjälp av välfärdsteknik.

Välfärdstjänster kännetecknas av användandet av ny teknik och av att flera olika aktörer kan vara inblandade i hanteringen av de enskildas uppgifter. Det innebär att det kan uppkomma risker på grund av bristande informationssäkerhet och bristande ansvarstagande för hanteringen – på samma sätt som dessa brister finns inom den övriga e-förvaltningen (se kapitel 11 om e-förvaltning och kapitel 22 om informationssäkerhet och integritet).

9.7 Kommitténs samlade bedömning av området

Hälso- och sjukvården

Tillgången till relevant information är en förutsättning för en god och säker hälso- och sjukvård för alla medborgare. Ett säkert och väl fungerande utbyte av information är en nödvändighet för att medborgarna ska få goda insatser i ett komplext system med många inblandade aktörer. Tillgång till nya informationstjänster har en stor potential att göra patienter långt mer delaktiga i sin vård. Ändamålsenliga och användbara informationssystem är också en förutsättning för att professionerna ska kunna använda sin kompetens och sin tid på det mest effektiva sättet. Funktionella informationssystem är en avgörande faktor för att vården ska kunna hantera framtidens utmaningar.

[35] SOU 2015:80.

Kommittén anser att ett gott integritetsskydd också är en nödvändig faktor för att åstadkomma en god och säker hälso- och sjukvård.

Det finns integritetsrisker förknippade med den digitala hanteringen av personuppgifter inom hälso- och sjukvården. Det är nödvändigt att utforma informationsutbytet inom och mellan vårdgivare på ett sådant sätt att det kan göras på ett säkert sätt. Vården måste såväl kunna uppfylla de krav på kvalitet som ställs på de medicinska insatserna som de som ställs på informationshanteringen.

Ökad kunskap, ledning och styrning ifråga om möjligheterna att hantera och utbyta information har stor betydelse för målsättningen att skapa en mer säker, ändamålsenlig och sammanhållen informationshantering inom hälso- och sjukvården. Enligt utredningen om rätt information i vård och omsorg[36] utgör okunskap om lagstiftningens möjligheter och avsaknad av aktiv rättstillämpning från vårdgivarnas sida en del av problemen med informationshanteringen i hälso- och sjukvården. Detta bekräftas av SLIT-rapporten 2015 som redogör för att det fortfarande återstår anpassning av system, regler och rutiner samt utbildning av personal för att uppfylla patientdatalagens krav.

Kommittén anser att det är anmärkningsvärt att lagen ännu inte implementerats fullt ut och Datainspektionen flera år efter patientdatalagens ikraftträdande, har hittat allvarliga och systematiska brister även hos stora och resursstarka vårdgivare.

Sammanfattningsvis konstaterar kommittén att risker uppstår i samband med informationshantering inom hälso- och sjukvården till följd av:

- bristande ledning och ansvarstagande över informationssystemen och de personuppgifter som hanteras i dessa,
- komplexa miljöer med många olika system för hantering av information,
- brist på gemensamma lösningar, t.ex. gemensam infrastruktur,
- bristande regelefterlevnad,
- bristande kunskaper hos både personal och ledning samt
- bristande informationssäkerhet.

[36] SOU 2014:23, s. 121 och s. 218 i bilaga 4.

I hälso- och sjukvården hanteras stora mängder känslig information om i stort sett hela befolkningen. Effekten av de brister vid hanteringen som iakttagits kan vara stora för enskilda individer och för hela befolkningen. Flera aktörer uppfyller ännu flera år efter att patientdatalagen trätt i kraft inte de krav på säkerhet som måste ställas vid hantering av känsliga personuppgifter. Mot denna bakgrund bedömer kommittén att det föreligger allvarliga risker för den personliga integriteten i samband med hantering av personuppgifter inom hälso- och sjukvården.

Välfärdsteknik och digitala tjänster inom socialtjänsten

Användning av olika digitala och tekniska lösningar i socialtjänsten såsom kameraövervakning, GPS-sändare och sensorer m.m. innefattar hantering av mycket närgångna och känsliga uppgifter om enskilda personer med stort hjälpbehov. Socialtjänsten berör stora delar av befolkningen. Det finns oklarheter i lagstiftningen om på vilket sätt personer med nedsatt beslutsförmåga kan erbjudas tjänster med hjälp av välfärdsteknik. Det finns också risker för bristande informationssäkerhet och bristande ansvarstagande för hur uppgifter hanteras. Kommittén bedömer sammantaget att det föreligger allvarliga risker för den personliga integriteten i samband med hantering av personuppgifter inom socialtjänstens användning av välfärdsteknik.

10 Forskning och statistik

Kommitténs bedömning: I samband med hantering av integritetskänsliga personuppgifter för forskningsändamål föreligger allvarlig risk för den personliga integriteten.

I samband med statens hantering av integritetskänsliga personuppgifter för statistikändamål föreligger viss risk för den personliga integriteten.

10.1 Företeelserna

Inom forskningen och statistikframställningen är personuppgifter av stor betydelse.

Digitaliseringen innebär att mängden uppgifter om enskilda personer totalt sett ökat kraftigt i samhället. Vidare har teknikutvecklingen gjort det möjligt att i realtid sambearbeta och analysera data från olika källor och i olika format. Utvecklingen har på så sätt radikalt förbättrat möjligheterna att samla in, använda sig av och sprida personuppgifter inom både forskningen och statistikverksamheten. Utvecklingen öppnar också för helt nya möjligheter: Inom statistikverksamheten är man t.ex. mycket intresserad av att kunna göra tillförlitlig statistik ner på hushålls- och individnivå av alla de nya datakällorna som uppstår när vardagslivet digitaliseras genom t.ex. sociala medier, sakernas internet (Internet of things), smarta elmätare osv.

Både inom forskningen och inom statistikframställningen rör det sig ofta om stora mängder uppgifter om den enskilde som var för sig eller sammantagna kan vara mycket integritetskänsliga. Det kan exempelvis vara frågan om uppgifter om hälsa, DNA och politiska åsikter, men även uppgifter om den enskildes sociala förhållanden såsom inkomst, arbete, boende, civilstånd och skuldsättning.

Även i de fall då varje uppgift i sig närmast är att anse som trivial ur ett integritetsperspektiv, är det med hjälp av de mycket stora statistikdatabaserna, där den absolut största uppgiftsmängden finns hos SCB, möjligt att följa en individ bokstavligen från vaggan till graven och skapa en mycket närgången bild av personen i fråga.

Sverige utmärker sig internationellt med sina stora och centraliserade myndighetsregister och statistikdatabaser som omfattar hela befolkningen i landet. Sverige utmärker sig också genom de unika personnumren som används konsekvent och genomgående av både myndigheter och företag. Personnumret möjliggör sambearbetning av data från många olika källor på ett sätt som inte skulle vara genomförbart i de flesta andra länder.

De stora myndighetsdatabaserna i Sverige utgörs till viss del av myndigheternas verksamhetssystem. Men härutöver har det allmänna också byggt upp stora datasamlingar som inte behövs som beslutsstöd i någon daglig verksamhet, utan som syftar till att möjliggöra forskning eller statistik. Exempel på sådana databaser är förstås all data som finns hos Statistiska centralbyrån (SCB), men även Socialstyrelsens hälsodataregister och vårdgivarnas nationella kvalitetsregister. Även om uppgifterna i dessa databaser i mycket stor utsträckning är hämtade från olika myndigheters och företags verksamhetssystem, hanteras uppgifterna alltså hos statistikmyndigheterna för helt andra syften än de verksamhetsrelaterade ändamål som föranledde den ursprungliga registreringen hos de myndigheter och företag som levererat uppgifterna till statistikmyndigheterna.

Det kan vara obligatoriskt eller frivilligt att som enskild person finnas med i en forsknings- eller statistikdatabas. Det är till exempel obligatoriskt att medverka med vissa uppgifter som samlas in inom vården i de s.k. hälsodataregistren. I andra register är medverkan frivillig, till exempel i nationella kvalitetsregister. Här behöver medverkan inte bygga på aktivt samtycke, utan på att den enskilde har rätt att säga nej till registrering (s.k. opt-out), vilket förutsätter att han eller hon först har blivit upplyst om registreringen och om rätten att stå utanför registret. Statistik som levereras från andra myndigheter och företag till SCB, kan den enskilde i regel inte avstå från att finnas med i. Det är dock frivilligt att medverka i undersökningar där SCB och andra statistikansvariga myndigheter vänder sig direkt till enskilda personer med enkäter och intervjuer. SCB har under de senaste åren rapporterat om en minskad benägenhet hos befolk-

ningen att delta i statistiska undersökningar.[1] Det kan leda till stora bortfall i undersökningarna, vilket i sin tur innebär att resultaten kan bli missvisande.

10.1.1 Statistik

Statistik som innehåller personuppgifter framställs inom många olika ämnesområden i samhället.

Det som sägs om statistik i detta kapitel, begränsar sig till statligt framtagen statistik, eftersom det i Sverige är staten som är den stora producenten av allmännyttig statistik som ska kunna delas med andra intressenter i samhället. Den statliga statistiken består dels av s.k. officiell statistik, dels av övrig statistik hos de statliga myndigheterna. För den officiella statistiken finns ett särskilt regelverk. Även övrig statlig statistik kan, under förutsättning att den har ett vidare syfte än att utgöra rent intern driftstatistik, omfattas av en del av detta regelverk.[2]

Det finns en stor efterfrågan på statistik i samhället, inte minst från myndigheter och från Regeringskansliet. Exempel på detta är den särlagstiftning som tillkommit för Institutet för arbetsmarknads- och utbildningspolitisk utvärdering (IFAU), och som behandlas närmare nedan, samt den omständigheten att SCB enligt senare års regleringsbrev ska leverera mikromaterial[3] till Regeringskansliet. Vidare har Riksrevisionen nyligen begärt åtkomst till flera olika mikrodatabaser hos SCB.[4]

Officiell statistik

Viss statistikframställning har staten ett särskilt ansvar för. Denna benämns officiell statistik och är reglerad i särskild lagstiftning. Enligt lagen (2001:99) om den officiella statistiken ska officiell statistik

[1] *Statistikskolan: Mer bortfall i statistiken*, SCB, http://www.scb.se/sv_/Hitta-statistik/Artiklar/Statistikskolan-Mer-bortfall-i-statistiken/ Hämtad 2016-05-12, samt Kristoffer Örstadius, *Sveriges officiella statistik hotar att bli missvisande*, publicerad på www.dn,se den 18 januari 2015.

[2] Statistikutredningens betänkandet *Vad är officiell statistik? En översyn av statistiksystemet och SCB*, SOU 2012:83.

[3] I detta fall statistiskt material som ska vara avidentifierat men som torde rymma goda möjligheter till bakvägsidentifiering.

[4] Riksrevisionens hemställan den 27 april 2016, dnr 2.3.4-2016-0688.

finnas för allmän information, utredningsverksamhet och forskning. Officiell statistik ska vara objektiv och allmänt tillgänglig. Regeringen har i förordningen (2001:100) om den officiella statistiken fastställt inom vilka områden det ska finnas officiell statistik och vilka myndigheter som ansvarar för denna (s.k. statistikansvariga myndigheter).

Personuppgifter samlas in för officiell statistik inom en rad olika samhällsområden. Ibland framställer den statistikansvariga myndigheten officiell statistik utifrån uppgifter som den samlar in i samband med sin egen verksamhet eller i myndighetsutövning i förhållande till enskilda. Ibland är det i stället andra verksamheter som rapporterar in uppgifter till den statistikansvariga myndigheten, som i sin tur bearbetar och sammanställer uppgifterna till officiell statistik. Några exempel:

- Försäkringskassan framställer officiell statistik om stöd till barnfamiljer och om stöd vid sjukdom och funktionsnedsättningar,
- Socialstyrelsen framställer officiell statistik om hälsa och sjukdomar, hälso- och sjukvård, dödsorsaker, individ- och familjeomsorg, äldre- och handikappomsorg samt om stöd och service till funktionshindrade,
- Statistiska centralbyrån framställer officiell statistik om bl.a. levnadsförhållanden, jämställdhet, vakanser och arbetslöshet, arbetstider, invandring och asylsökande, inkomster och inkomstfördelning och om hushållens utgifter.

Även känsliga personuppgifter får behandlas av myndigheterna vid framställningen av ovannämnda kategorier av officiell statistik.

Det finns 27 statistikansvariga myndigheter. Av dessa är det SCB som sitter på den avgjort största samlingen av data på individnivå. Vidare är det SCB som ansvarar för sektorsövergripande statistik såsom arbetsmarknads-, befolknings-, ekonomisk, välfärds- och viss utbildningsstatistik. SCB ansvarar också för att samordna det statliga statistiksystemet och överlämnandet av statistiska uppgifter till internationella organisationer. Övriga statistikansvariga myndigheter ansvarar för officiell statistik inom sina respektive samhällssektorer eller motsvarande.

Övrig statistik

Utöver den officiella statistiken tas det också fram mycket annan statistik i Sverige, inom såväl privat som offentlig sektor.

Statistikutredningen konstaterade att i stort sett samtliga statistikansvariga myndigheter utöver sin officiella statistik, även tar fram annan statistik av allmäninformativ karaktär och ger den i stort sett samma spridning som den officiella statistiken.[5] Det kan handla om bearbetningar av myndighetens officiella statistik, t.ex. nedbrytningar på lägre geografiska nivåer, som då inte klassas som officiell statistik. Men det kan också handla om annan återkommande statistik, som myndigheten har valt att inte (ännu) göra till officiell statistik. I det senare fallet kan det röra sig både om statistik som producerats under lång tid och om nyare statistikprodukter.

Omfattningen av denna övriga statistik varierar mycket mellan myndigheterna, allt från att den är betydligt mer omfattande än den officiella statistiken, till att den utgör en klart mindre del. Statistikutredningen kunde inte göra sig någon exakt bild av hur omfattande denna verksamhet hos myndigheterna var. Myndigheterna hade själva svårt att ge en exakt siffra till Statistikutredningen avseende den totala statistikverksamhet som de bedriver.

Även statliga myndigheter som i lagens mening inte är statistikansvariga, tar fram statistik om sina ansvarsområden. Även här varierar omfattningen från myndighet till myndighet. Några av myndigheterna anser att deras statistik borde ingå i den officiella statistiken. Det finns dock ingen övergripande sammanställning över den här statiskverksamhetens omfattning och natur.

10.1.2 Forskning

När personuppgifter hanteras för forskningsändamål, hämtas uppgifterna från olika myndighetsregister, från den officiella statistiken, från kvalitetsregister, från biobanker eller ur särskilda forskningsregister.[6] I en del studier inhämtar forskarna alla, eller vissa uppgifter direkt från enskilda personer.

[5] Statistikutredningen genomförde en egen enkätundersökning för att få någon klarhet i frågan, SOU 2012:83, s. 146 ff.

[6] Registerforskningsutredningens betänkande *Unik kunskap genom registerforskning*, SOU 2014:45, s. 306 f.

Ett godkännande från en etikprövningsnämnd krävs om man inom ramen för ett forskningsprojekt kommer att hantera känsliga personuppgifter eller personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.[7] Om inga sådana personuppgifter kommer att hanteras inom projektet, krävs godkännande från en etikprövningsnämnd endast om det rör sig om viss typ av forskning.[8] För en del forskningsprojekt där visserligen personuppgifter kommer att hanteras, men inga uppgifter enligt 13 eller 21 §§ personuppgiftslagen, krävs således inte något tillstånd från en etikprövningsnämnd.

I många fall där känsliga personuppgifter enligt 13 § personuppgiftslagen kommer att hanteras, men där forskarna inte har någon direkt kontakt med personerna, vilkas uppgifter ska undersökas i projektet, tillåter etikprövningsnämnderna att forskning bedrivs utan att de enskilda ges någon information om att deras uppgifter används i forskningen och utan att deras samtycke behöver inhämtas.

Varje år inleds ett stort antal forskningsprojekt i landet. Exempelvis avgjordes under år 2014 totalt 5 636 ärenden i de regionala etikprövningsnämnderna.[9] Forskningen kan bedrivas av företag, av statliga eller kommunala myndigheter eller av andra slags organisationer.

Inom forskningen är internationella samarbeten inte ovanliga, vilket även kan innebära att personuppgifter från Sverige delas med forskargrupper i andra länder.[10]

---

[7] Det vill säga, att tillstånd krävs om det rör sig om personuppgifter enligt 13 eller 21 §§ personuppgiftslagen.

[8] Tillstånd krävs om det rör sig om forskning som 1. innebär ett fysiskt ingrepp på en forskningsperson, 2. utförs enligt en metod som syftar till att påverka forskningspersonen fysiskt eller psykiskt eller som innebär en uppenbar risk att skada forskningspersonen fysiskt eller psykiskt, 3. avser studier på biologiskt material som har tagits från en levande människa och kan härledas till denna människa, 4. innebär ett fysiskt ingrepp på en avliden människa, eller 5. avser studier på biologiskt material som har tagits för medicinskt ändamål från en avliden människa och kan härledas till denna människa.

[9] Budgetpropositionen 2016, förslag till statens budget för 2016, finansplan och skattefrågor, prop. 2015/16:1.

[10] Ibland t.o.m. som handelsvara i utbyte mot ekonomiskt stöd för forskningsgrupperna: En rapport framtagen för regeringen och SKL inleds med ett fiktivt scenario där USA betalar 10 miljarder dollar per år bl.a. för att få tillgång till uppgifter från svenska kvalitetsregister. *Guldgruvan i hälso- och sjukvården, Förslag till gemensam satsning 2011–2015*, författad av Måns Rosén. Upplägget med forskningsfinansiering i utbyte mot data är redan i dag en realitet. Det fiktiva i scenariot är bidragets och satsningens omfattning. I rapporten beskrivs hur svenska register kan användas för att locka industriinvesteringar till Sverige. Ett annat, nationellt exempel på data som ekonomisk tillgång inom hälso- och sjukvården och forskningen, är statens ersättning till vårdgivare för varje patient som registreras i vissa kvalitetsregister.

10.2 Det skyddande regelverket

I EU:s dataskyddsdirektiv behandlas både statistikverksamhet och forskning särskilt fördelaktigt. Dessa verksamheter ges undantag från vissa av de grundläggande kraven på behandlingen, t.ex. beträffande hur länge uppgifter får sparas och möjligheten att använda uppgifter för nya ändamål. Bägge dessa undantag förutsätter dock att medlemsstaterna beslutar om eller vidtar lämpliga skyddsåtgärder. Direktivets bestämmelser i detta hänseende har genomfört i Sverige genom i första hand personuppgiftslagen (1998:204).

Personuppgiftsbehandling i samband med sådan forskning eller statistikframställning som behandlas i detta kapitel, regleras av ett flertal bestämmelser i olika lagar, vilka i huvudsak är:

- personuppgiftslagen,
- lagen (2003:460) om etikprövning av forskning som avser människor,
- lagen om den officiella statistiken,
- lagen (1998:543) om hälsodataregister,
- lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.

Beroende på vilken slags forskning eller statistikframställning det är frågan om, kan personuppgifter hanteras under vitt skilda förutsättningar; alltifrån helt utan den enskildes vetskap, till att det krävs ett uttryckligt och informerat samtycke från varje forskningsperson.

Något förenklat kan sägas att forsknings- och statistikprojekt regleras av personuppgiftslagen och lagen om etikprövning av forskning som avser människor. För uppbyggnaden av mer permanenta datakällor krävs stöd i särskild författning, såsom ovan nämnda lagar eller den särskilda lagen för Institutet för arbetsmarknads- och utbildningspolitisk utvärdering som berörs nedan – lagen (2012:741) om behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering.

10.3 Risker för den personliga integriteten

Datainspektionen har under de senaste åren granskat en rad forskningsprojekt, en forskningsdatabas och flera författningsförslag angående upprättandet av permanenta forsknings- eller statistikdatabaser.

När det gäller forskningsprojekt, har Datainspektionens tillsyn visat att det inte sällan förekommer brister i forskningsprojekt avseende hur forskningshuvudmännen informerar de personer som ingår i forskningen om hur deras uppgifter kommer att användas och vilka rättigheter de har. Det framkom i slutredovisning i december 2012 och juli 2015 av ett flertal tillsynsärenden.[11] Ett särskilt uppmärksammat ärende hos Datainspektionen rörde ett klagomål från en förälder vars 11-åriga dotter hade deltagit i en forskningsstudie som bedrevs i skolan av ett universitet, utan att vårdnadshavarna hade informerats eller lämnat sitt samtycke. I forskningsstudien samlades det in både personuppgifter och hårstrån från barnen i skolan. Datainspektionen fann att universitet behandlade personuppgifter i strid med personuppgiftslagen.[12] Datainspektionens tillsyn visar också att det i forskningsprojekt kan råda osäkerhet om vem som är ytterst ansvarig för de personuppgifter som samlas in (slutredovisning i januari 2011 av bred tillsynsinsats).[13]

I tillsynen av en forskningsdatabas vid Karolinska institutet (den s.k. Lifegene-databasen) år 2011 kom Datainspektionen fram till att insamlingen av personuppgifter måste upphöra eftersom ändamålen med databasen var för otydliga och därmed inte uppfyllde personuppgiftslagens krav. Enligt personuppgiftslagen måste den som registreras i den här typen av databaser få reda på hur personuppgifterna som samlas in kommer att användas och därefter ge sitt medgivande till att uppgifterna registreras. I den aktuella databasen hade man angivit att syftet var att använda uppgifterna för ”framtida forskning”, vilket Datainspektionen ansåg inte gav de medverkande personerna någon reell möjlighet att bilda sig en uppfattning om hur uppgifterna

[11] *Forskningsprojekt dåliga på att informera*, Datainspektionen 2012, http://www.datainspektionen.se/ press/nyheter/2012/forskningsprojekt-daliga-pa-att-informera/ Hämtat 2016-05-12. Samt *Tydligare information krävs vid forskningsstudier*, Datainspektionen 2015, http://www.datainspektionen.se/press/nyheter/2015/tydligare-information-kravs-vid-forskningsstudier/ Hämtat 2016-05-12.

[12] Datainspektionens beslut den 3 oktober 2011 i dnr 1938-2010.

[13] *Forskare lyssnar på Datainspektionen men har inte alltid koll på ansvarsfrågan*, Datainspektionen 2011, http://www.datainspektionen.se/press/nyheter/2011/forskare-lyssnar-pa-datainspektionen-men-har-inte-alltid-koll-pa-ansvarsfragan/ Hämtat 2016-05-12.

faktiskt skulle komma att användas och spridas. Ändamålet var därför för allmänt hållet. Datainspektionen menade också att register som har som ambition att omfatta stora delar av befolkningen sedan lång tid tillbaka brukar regleras i särskilda författningar (registerförfattningar) vid sidan av såväl den tidigare datalagen som personuppgiftslagen. På grund av sådana registers omfattning eller känsliga innehåll har det ansetts rimligt att riksdagen eller regeringen ska få ta ställning till såväl inrättandet av registren som omfattningen.[14]

Med anledning av Datainspektionens granskning, beslutade riksdagen år 2013 om en tidsbegränsad speciallagstiftning i syfte att möjliggöra allmänna forskningsdatabaser: lagen om vissa register för forskning om vad arv och miljö betyder för människors hälsa. Av lagen framgår bl.a. att personuppgifter får behandlas för ändamålen att skapa underlag för olika forskningsprojekt om vad arv och miljö betyder för uppkomsten och utvecklingen av olika typer av sjukdomar och för människors hälsa i övrigt.

I frågan om förlängning av den tidsbegränsade speciallagstiftningens giltighet, har Datainspektionen yttrat sig kritiskt.[15] Det som Datainspektionen anför, är i huvudsak att ändamålsbestämmelserna i den aktuella lagen inte är förenliga med dataskyddsdirektivets krav på att ändamål ska vara särskilda och uttryckligt angivna. Datainspektionen stöder sin ståndpunkt på ett uttalande från Artikel-29-gruppen, enligt vilket ”framtida forskning” vanligtvis är en för allmänt hållen ändamålsformulering. I sammanhanget har Datainspektionen även lyft fram att möjligheten till att upprätta allmänna forskningsdatabaser innebär att datainsamling för forskningsändamål i många fall inte längre kommer att behöva prövas av en etikprövningsnämnd. Forskare kan i stället samla in uppgifter utan godkännande. Först i ett senare skede, när uppgifterna ska börja användas i ett visst forskningsprojekt kommer det att behövas ett etikgodkännande. Det innebär i praktiken en ändring av den hittillsvarande ordningen att etikprövningsnämnderna även ska pröva om och i så fall hur personuppgifter får samlas in från forskningspersonerna.

Trots Datainspektionens invändningar, beslutade riksdagen år 2015 att lagen om vissa register för forskning om vad arv och miljö betyder för människors hälsa, som gällde till utgången av 2015, ska fortsätta att

[14] Datainspektionens beslut den 16 december 2011 i dnr 766-2011.
[15] Datainspektionens beslut om yttrande den 21 mars 2015 i dnr 596-2015.

gälla till och med den 31 december 2017. I ett register enligt den tidbegränsade lagen, får det endast ingå personuppgifter som den enskilde själv har lämnat i syfte att uppgifterna ska ingå i registret.

Samtidigt som den tidsbegränsade lagstiftningens giltighet förlängts, har Registerforskningsutredningen lämnat ett betänkande med förslag till permanent reglering av forskningsdatabaserna.[16] Till skillnad mot den nu gällande, tidsbegränsade lagstiftningen (där samtycke är ett villkor för all hantering) ska det enligt förslaget vara möjligt för statliga myndigheter att utan stöd av samtycke, utan att någon information lämnas till de enskilda och utan godkännande av en etikprövningsnämnd, samla in och lagra känsliga uppgifter från en rad olika datakällor. I betänkandet ges exempel på den uppsjö av myndighetsregister från vilka uppgifter skulle kunna inhämtas till de forskningsdatabaser som förslaget skulle möjliggöra. Här nämns bl.a. myndigheternas register för administrativa ändamål, såsom skatteregistret med taxerade och pensionsgrundande inkomster, Centrala studiestödsnämndens register över personer som får studiestöd eller har studieskulder och Försäkringskassans socialförsäkringsdatabas med uppgifter om olika förmåner och bidrag. Vidare nämns de register som finns hos SCB och de 26 andra statistikansvariga myndigheterna som har i uppdrag att producera officiell statistik. Hos dessa hanteras, som framgått ovan, uppgifter om bl.a. hushållens ekonomi (inkomster och inkomstfördelning, hushållens utgifter), uppgifter från hälso- och sjukvården (hälsa och sjukdomar, dödsorsaker), uppgifter från rättsväsendet (uppgifter om brott, kriminalvård, återfall i brott) m.m.

I remissbehandlingen av betänkandet, avstyrkte Datainspektionen förslaget, med motiveringen att det inte är förenligt med 2 kap. 6 § andra stycket regeringsformen. Förslaget riskerar enligt Datainspektionen att leda till betydande integritetsintrång genom att tillåta omfattande insamling av personuppgifter utan att ändamålen är tillräckligt specificerade och utan att kräva integritetsskyddande åtgärder som uppväger integritetsintrånget. Vidare anförde Datainspektionen att förslaget innebär att alla typer av personuppgifter kommer att kunna samlas in för forskningsändamål som inte är tydligt avgränsade

[16] *Unik kunskap genom registerforskning*, SOU 2014:45.

eller specificerade. Förslaget möjliggör därmed enligt Datainspektionen en närgången kartläggning av enskildas privatliv, familjeförhållanden, sjukdomshistoria, arbetsliv, brottsuppgifter m.m.

När det gäller statistikdatabaser, har Datainspektionen uttryckt oro för att vissa myndigheter vill bygga upp egna samlingar med uppgifter om medborgarna för forskningsändamål, parallellt till de samlingar som redan finns hos de statistikansvariga myndigheterna. Ett exempel på detta är Institutet för arbetsmarknads- och utbildningspolitisk utvärdering (IFAU) som t.o.m. fått ett särskilt lagstöd för egna samlingar av känsliga personuppgifter. Från början var lagstödet tidsbegränsat men det gäller numera tills vidare. I sitt remissvar till lagförslaget ifrågasatte Datainspektionen IFAU:s behov av att bygga upp egna samlingar av personuppgifter som redan bevaras med lagstöd hos andra myndigheter t.ex. SCB och Arbetsförmedlingen. Det var enligt Datainspektionens mening inte önskvärt ur integritetsskyddssynpunkt att statliga myndigheter bygger upp parallella samlingar med uppgifter om medborgarna.[17] Även SCB har yttrat sig kritiskt i det aktuella lagstiftningsärendet.[18]

De redovisade ärendena ger en bild av området som kännetecknas av en strävan hos vissa myndigheter och utredningar som sysslar med statistik och forskning att så långt som möjligt underlätta hanteringen av personuppgifter, samtidigt som den integritetsskyddande lagstiftning ses som ett hinder för den verksamheten.[19]

Ett annat exempel från tillsynen är Datainspektionens granskning av ett forskningsprojekt vid Stockholms universitet.[20] Vetenskapsrådet hade i ett tidigare skede prövat om det aktuella projektet skulle beviljas anslag, och då kommit in på den omständigheten att Datainspektionen redan flera år tidigare (1986 i det s.k. Metropolitärendet) faktiskt hade beslutat att datasamlingen ifråga skulle avidentifieras och att inga fler uppgifter skulle tillföras datasamlingen, vilket sammantaget skulle omöjliggöra framtida forskning på materialet. Forskningshuvudmannen ville trots detta forska på materialet,

[17] Datainspektionens beslut om yttrande den 21 mars 2012 i dnr 192-2012.

[18] SCB:s beslut om yttrande den 17 december 2014 i dnr 2014/1464.

[19] Några exempel utöver de som redan nämns: betänkandena *Registerdata för forskning* (SOU 2012:36), *Vad är officiell statistik? En översyn av statistiksystemet och SCB*, SOU 2012:83, *Unik kunskap genom registerforskning,* SOU 2014:45. Ett annat exempel på detta är rapporten Översyn av de nationella kvalitetsregistren: Guldgruvan i hälso- och sjukvården – förslag till gemensam satsning 2011–2015, författad av Måns Rosén.

[20] Datainspektionens beslut i dnr 1776-2010.

återpersonifiera det så långt som möjligt och påföra nya datasamlingar. Kring denna frågeställning resonerade Vetenskapsrådet i ett särskilt PM, men kom fram till att anslagsansökan skulle beviljas eftersom ett beslut om avslag med hänvisning till legala oklarheter skulle innebära att ”man använder andra kriterier i bedömningen av detta ärende än av andra”.

Vetenskapsrådet har även i andra sammanhang utmärkt sig genom att bortse från juridisk problematik kopplad till integritetsskyddet, exempelvis när rådet år 2005 rekommenderade regeringen att anslå medel för Svensk nationell datatjänst (SND) vid Göteborgs universitet – i full vetskap om att själva grundupplägget med SND stred mot gällande rätt.[21] Vetenskapsrådets bedömning att verksamheten saknar lagstöd bekräftades år 2012 när Datainspektionens förelade Göteborgs universitet att upphöra med insamling och övrig behandling av personuppgifter i material insamlat inom ramen för Svensk nationell datatjänst.[22]

Det är flera olika lagar som reglerar och samverkar om hur känsliga personuppgifter får hanteras för forsknings- eller statistikändamål. Regelverket kan många gånger vara svårt att överblicka och förstå även för dem som är professionellt verksamma inom området.

10.4 Kommitténs samlade bedömning av området

Den övergripande bilden av området är att svenska myndigheter förfogar över ett betydande antal databaser för forsknings- och statistikändamål som tillsammans täcker hela landets totala befolkning. På så sätt utmärker sig Sverige – det finns inte många andra länder som kan jämföra sig med oss när det gäller möjligheten för det allmänna att undersöka sina invånares liv.

[21] Vetenskapsrådet gjorde denna analys av rättsläget i samma rapport där man föreslog att regeringen skulle satsa 10 miljoner kronor på uppbyggandet av SND. Rapporten *Om forskningens infrastrukturer inom humaniora och samhällsvetenskap i Sverige*, april 2005, Vetenskapsrådets dnr 131-2004-8236, s. 20.

[22] Datainspektionens beslut den 18 april 2012 i dnr 811-2011. Beslutet överklagades, men förvaltningsrätten avslog klagomålet, Förvaltningsrättens i Stockholm dom den 14 oktober 2013 i mål nr 9987-12. Domen har vunnit laga kraft.

Det finns både inom forskningen och inom statistikverksamheten ett stort intresse för att dra nytta av att allt mer data genereras om enskilda och att det samtidigt har blivit möjligt att sammanföra och analysera data från varierande datakällor.

Inom forskningen rör det sig ofta om stora samlingar uppgifter som kan vara synnerligen integritetskänsliga. Inte sällan får uppgifterna hanteras utan information till den enskilde och utan samtycke från denne. Den enskilde har i dessa fall små möjligheter att påverka hur uppgifterna används. De samtycken som inhämtas kan ibland vara mycket breda och endast ge den enskilde en diffus uppfattning om hur uppgifterna faktiskt kan komma att hanteras. Uppgifterna kan också komma att spridas utan den enskildes vetskap. Vidare är det många olika huvudmän med varierande kunskap om integritetsskydd som bedriver forskning. Tillsynen visar också på vissa återkommande brister i hanteringen av personuppgifter inom forskningsprojekt. Sammantaget anser kommittén därför att hantering av integritetskänsliga personuppgifter för forskningsändamål innebär en allvarlig risk för den personliga integriteten, särskilt när uppgifterna hanteras utan stöd av samtycken eller med stöd av samtycken som är brett formulerade eller som lämnats tidigare i livet.

Även inom den statliga statistikverksamheten rör det sig ofta om stora samlingar uppgifter som kan vara integritetskänsliga. Inte sällan får uppgifterna hanteras utan information till den enskilde och utan samtycke från denne. Den enskilde har i dessa fall inga möjligheter att påverka hur uppgifterna används. Officiell statistik produceras av en rad olika statliga myndigheter, vilka måste kunna skilja mellan hantering av uppgifter i myndighetens kärnverksamhet, och hanteringen inom myndighetens statistikverksamhet. Landets största och känsligaste statistikdatabaser finns emellertid hos två statliga myndigheter: SCB och Socialstyrelsen. Hos dessa två finns tämligen goda förutsättningar att kontrollera hur uppgifterna lagras, lämnas ut och används. Det finns också särskild lagstiftning för den statistikrelaterade hanteringen av personuppgifter hos dessa två och hos övriga statistikansvariga myndigheter. Det saknas tillsynsrapporter som vittnar om brister i samband med statistikverksamhet hos någon statlig myndighet när det gäller integritetsskyddet. Sammantaget anser kommittén att statens hantering av integritetskänsliga personuppgifter för statistikändamål innebär en viss risk för den personliga integriteten.

Samtidigt måste beaktas, beträffande såväl forskning som den statliga statistikverksamheten, att resultaten av dessa verksamheter bidrar med viktiga värden inom en rad olika samhällsområden. Verksamheterna är ur ett samhällsperspektiv mycket viktiga för att kunna planera och utvärdera reformer, för att skapa transparens i samhällsstyret och för att ge bättre underlag för analys, debatt och beslut.

11 E-förvaltning

Kommitténs bedömning: De olika företeelser som vi har kartlagt inom området e-förvaltning är förknippade med risker av olika allvarlighetsgrad; såväl vissa risker som påtagliga och allvarliga risker kan konstateras. Läs mer om hur vi bedömt riskerna avseende de olika företeelserna i avsnitt 11.3.

11.1 Företeelser

11.1.1 Avgränsning

Begreppet e-förvaltning definieras ofta som ”verksamhetsutveckling i offentlig förvaltning som drar nytta av informations- och kommunikationsteknik kombinerad med organisatoriska förändringar och nya kompetenser”.[1]

Det rör sig om digitala tjänster som används i kommunikationen mellan myndigheter och enskilda personer eller företag, mellan olika myndigheter eller inom en och samma myndighet.

E-förvaltningen inom skolan och hälso- och sjukvården behandlas i respektive kapitel (kapitel 7 och 9).

Offentlig förvaltning är en storkonsument av personuppgifter. Myndigheterna använder ofta uppgifterna i sammanhang som är viktiga för den enskilde, t.ex. för att bestämma rättigheter och skyldigheter.

[1] E-delegationens betänkande *Organisering av framtidens e-förvaltning*, SOU 2013:75.

11.1.2 Ökad insamling, spridning och användning av personuppgifter

De senaste åren har det skett en successiv och bred utveckling av e-förvaltningen, föranledd bl.a. av krav från regeringen på effektivisering av förvaltningen och på önskemål från enskilda och företag. Det har kommit allt fler e-tjänster för medborgarna, såsom digitala möjligheter att deklarera, ansöka om föräldrapenning och ansöka om förskoleplats m.m. Det blir också allt vanligare att myndigheter vill dela uppgifter med varandra. Det digitala uppgiftsflödet till och mellan myndigheterna har således ökat på flera olika sätt.

Nästan sju av tio personer (69 procent) i åldern 16–74 år hämtade information från myndigheters webbplatser enligt Statistiska centralbyråns undersökning för år 2015.[2] I motsvarande undersökning för år 2014 var resultatet på samma fråga 79 procent.[3]

I en enkätundersökning som gjordes i samband med utvecklingen av e-tjänsten Mina meddelanden, uppgav 84,5 procent av de svarande att de tyckte att det är mycket eller ganska intressant att samla kommunikationen med myndigheterna elektroniskt på ett och samma ställe.[4] I fråga om i vilket format respondenten föredrog att få information från myndigheterna, så föredrog 32,7 procent att få myndighetsmeddelanden i pappersformat. För 41,7 procent var elektronisk form att föredra och för 25,6 procent spelade det ingen roll.

Resultatet av undersökningen visade också att det bland de svarande fanns en uppfattning om att säkerheten är viktig när det gäller åtkomsten till myndighetsmeddelande. Av de svarande tyckte 75 procent att det är mycket viktigt att ingen obehörig kommer åt meddelandena. Det ställdes också frågor om myndigheters användning av enskildas mobiltelefonnummer. De svarande visade sig vara mycket ovilliga att sprida sina mobiltelefonnummer till andra än myndigheterna. Bara fem procent gick med på detta. Sedan var de svarande kluvna till om mobilnumret ska få användas av myndigheterna förutom för sms-avisering.

---

[2] SCB:s statistik *Vad gör personer i åldern 16–74 år vid kontakt med myndigheter via Internet.*

[3] SCB känner inte till varför antalet respondenter som svarat att de hämtat information, har minskat.

[4] *Behovsanalys privatperson 2012 A, Mina meddelanden, En förvaltningsgemensam infrastrukturtjänst*, Utredningsrapport från Verksamt.se med dnr 131-665930-12/123.

När Delegationen för e-förvaltning[5], härefter kallad E-delegationen, år 2013 genomförde sin sista uppföljning av de statliga myndigheternas arbete med e-förvaltning och e-tjänster, visade det sig att de 137 myndigheter som medverkade i uppföljningen tillhandahöll sammantaget 3 816 e-tjänster till privatpersoner, företag och offentlig sektor. Av dessa tillhandahålls 1 057 tjänster via gränssnittet maskin-till-människa och 2 183 tjänster via gränssnittet maskin-till-maskin. Elektroniskt informationsutbyte mellan de statliga myndigheterna (maskin-till-maskin) hade ökat markant jämfört med motsvarande undersökning år 2011. Betydligt fler statliga myndigheter var också involverade i gemensamma satsningar jämfört med år 2011.[6]

Ökningen beror bl.a. på att såväl verksamheterna som regelverk och teknik har utvecklats för att möjliggöra ett utökat utbyte av uppgifter över myndighetsgränserna. Exempel på detta är de bestämmelser som trädde i kraft år 2009 och som innebär ett utökat elektroniskt informationsutbyte mellan myndigheter.[7] Information ska huvudsakligen utbytas genom s.k. direktåtkomst.

Förändrad lagstiftning

En konkret tillämpning av 2009 års regeländringar är den s.k. LEFI Online (LEverera FörmånsInformation) som är en e-tjänst för uppgiftsutlämnande från Försäkringskassan. Genom LEFI Online lämnar Försäkringskassan ut person- och förmånsinformation till mottagare som har rätt att få ta del av informationen. Målgruppen för tjänsten är externa parter som försäkringsbolag, kommuner (huvudsakligen socialnämnder) och statliga myndigheter.

Frågan om direktåtkomst i LEFI Online har prövats av Högsta förvaltningsdomstolen.[8] Domstolen kom fram till att socialnämndernas åtkomst i systemet inte är att betrakta som direktåtkomst enligt socialförsäkringsbalken (2010:110), eftersom socialnämn-

[5] Dir. 2009:19.

[6] *Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2013*, Rapport från E-delegationen daterad den 5 november 2013.

[7] Regeringens proposition *Utökat elektroniskt informationsutbyte*, prop. 2007/08:160.

[8] Högsta domstolens dom en 29 oktober 2015 i mål nr 1356-14. Frågan om direktåtkomst är i många författningar särskilt reglerad, eftersom direktåtkomst kan innebära att uppgifter blir åtkomliga för ett stort antal personer och organisationer utanför den egna.

derna inte på egen hand kan söka information i socialförsäkringsdatabasen och eftersom ett utlämnande genom LEFI Online förutsätter att Försäkringskassan reagerar på en begäran om att de efterfrågade uppgifterna ska lämnas ut. Datainspektionen anser att det utifrån domstolens resonemang är oklart vilket utrymme det överhuvudtaget finns att beteckna ett elektroniskt utbyte mellan myndigheter som direktåtkomst.[9]

Ett annat exempel på konkret tillämpning av regeländringarna är E-delegationens projekt, *Effektiv informationsförsörjning – ekonomiskt bistånd*, som resulterade i en teknisk lösning för samordning av socialnämndernas direktåtkomst i ärenden om försörjningsstöd. Tjänsten har numera tagits i fullt bruk. Genom tjänsten kan handläggare inom socialtjänstens verksamhetsområde för ekonomiskt bistånd få utlämnat information från a-kassorna, Arbetsförmedlingen, Centrala studiestödsnämnden, Försäkringskassan, Pensionsmyndigheten och Skatteverket. Försäkringskassan ansvarar för teknisk förvaltning och drift av tjänsten på uppdrag av Sveriges Kommuner och Landsting (SKL).[10]

Teknisk utveckling

Ett exempel på teknisk utveckling som möjliggjort ett ökat digitalt utbyte av personuppgifter är det s.k. Spridnings- och hämtningssystemet, SHS. SHS är en s.k. informationsväxel och ett sätt för att utbyta information digitalt. SHS används i dag av statliga myndigheter, kommuner och landsting, men även av företag och organisationer vid informationsutbyte. Det används bl.a. för att skicka elektroniska dokument till myndigheter, hämta information från andra myndigheters datasystem, prenumerera på information från andra myndigheter, ställa frågor till en annan myndighet samt för att besvara dessa frågor. Det är Försäkringskassan som förvaltar SHS-konceptet med tillhörande ramverk.

[9] Datainspektionens remissvar den 20 november 2015 avseende SOU 2015:39, myndighetens dnr 1125-2015.

[10] E-delegationens slutbetänkande *En förvaltning som håller ihop*, SOU 2015:66.

Organisationsfrågor

De senaste årens myndighetssammanslagningar har också medfört ökade möjligheter att utan hinder av registerförfattningar eller sekretess dela uppgifter, som tidigare inte fick delas över myndighetsgränserna. Exempel på detta är de allmänna försäkringskassorna som ombildats till Försäkringskassan som numera tillsammans utgör en enda myndighet, samt de lokala skattemyndigheterna som slagits samman till myndigheten Skatteverket. Sekretess gäller dock fortfarande mellan självständiga verksamhetsgrenar inom en myndighet. Även bildandet av helt nya myndigheter som hos sig samlar funktioner från flera andra myndigheter innebär en ökad spridning och samtidigt en större ansamling av personuppgifter hos den nya myndigheten. Ett exempel på detta är bildandet av Statens servicecenter som genom att ta över vissa personaladministrativa arbetsuppgifter från andra myndigheter hanterar uppgifter om ett stort antal statligt anställda i en central databas.

På den kommunala sidan finns det stor frihet för kommunfullmäktige att besluta vilka nämnder som ska finnas Därmed har kommunerna även långtgående möjligheter att bestämma hur sekretessgränserna ska dras i den egna organisationen.[11] Eftersom kommunerna själva bestämmer vilka nämnder de vill ha, ser det olika ut runt om i Sverige. I ett antal kommuner har man under senare år förändrat sin politiska organisation på ett genomgripande vis. Den traditionella politiska organisationen med facknämnder har här i stora drag ändrats till en organisation som bygger på fullmäktigeberedningar och styrelseutskott. De icke-obligatoriska sektorsansvariga nämnderna har tagits bort. Förutom styrelsen, valnämnden, och i förekommande fall överförmyndarnämnd finns endast en eller ett par myndighetsnämnder kvar.[12]

[11] Sekretesskyddets beroende av kommunernas val av organisationsform har kritiserats och utretts, men inte ändrats (Geijer, Lenberg, Tansjö, Offentlighets- och sekretesslagen, 1 juli 2015, Zeteo, kommentaren till 8 kap. 2 §).

[12] Rapporten *Alternativa politiska organisationer*, Sveriges kommuner och landsting, juni 2009.

Dubblering av databaser

Dubbleringar av andra myndigheters databaser innebär också en ökad hantering av personuppgifter hos myndigheterna. Ett exempel på detta är den uppgiftssamling som byggts upp vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering (IFAU). Uppgiftssamlingen finns redan i allt väsentligt hos Statistiska centralbyrån. Regeringen har dock ansett att IFAU:s behov av personuppgifter inte kan tillmötesgås genom de tekniska lösningar avseende direktåtkomst till statistikuppgifter och innehåll hos Statistiska centralbyrån som står till buds. Datainspektionen har reagerat mot detta och menar att en sådan möjlighet att bygga upp egna samlingar av personuppgifter som redan med lagstöd bevaras hos andra myndigheter, som t.ex. hos Statistiska centralbyrån, inte bör finnas.[13]

En variant av dubbleringar av databaser, är när myndigheter får s.k. bruttoaviseringar. Bruttoaviseringar innebär att en myndighet som hanterar uppgifter om enskilda och vill uppdatera dessa uppgifter, begär att få ta del av samtliga uppgifter i en central databas som även innehåller uppgifter om andra personer än de som är aktuella hos myndigheten. Det kan vara ett effektivare och enklare sätt att uppdatera en databas jämfört med att endast ta del av ett urval hos den centrala myndigheten som sitter på de uppdaterade uppgifterna. Exempel på detta är när vissa myndigheter ska uppdatera sina befolkningsregister med hjälp av Statens personadressregister (SPAR). SPAR är ett offentligt register som omfattar alla personer som är folkbokförda i Sverige, både svenska och utländska medborgare. Uppgifterna i SPAR uppdateras varje dygn med uppgifter från folkbokföringsregistret. Syftet med SPAR är att lämna ut uppgifter elektroniskt under förutsättning att mottagaren uppfyller vissa villkor. De uppgifter som finns i SPAR är namn, person- eller samordningsnummer, födelsetid, adress, folkbokföringsort, födelsehemort, svenskt medborgarskap, make eller vårdnadshavare, avregistrering från folkbokföringen på grund av dödsfall eller annan anledning, summan av fastställd inkomst och inkomst av kapital, ägare av småhus- eller lantbruksenhet med småhus på tomtmark samt uppgift om kommun, taxeringsvärde för småhusenhet samt information om den registrerade begärt spärr mot direktreklam med SPAR som

[13] Datainspektionens remissvar på regeringens förslag om fortsatt giltighet av lagen (2012:741) om behandling av personuppgifter vid IFAU, Datainspektionens dnr 2468-2014.

adresskälla. Av förordningen (1998:1234) om det statliga personadressregistret framgår att bruttoavisering får medges den som i sin verksamhet regelmässigt behandlar uppgifter om en betydande del av befolkningen och fortlöpande behöver uppdatera dessa. Möjligheten till bruttoavisering infördes i förordningen med viss tveksamhet om detta alltid var i överensstämmelse med dataskyddsdirektivet och personuppgiftslagen (1998:204).[14]

Bruttoaviseringar har även diskuterats beträffande uppdateringar av personuppgifter i e-tjänsten Mina meddelanden. När det gäller den tjänsten är massutlämnanden inte författningsreglerade på samma sätt som för SPAR. Teknikutvecklingen går emellertid allt mer ifrån bruttoaviseringar, till att bygga på lösningar där systemen kommunicerar genom frågor och svar.

Samverkan mellan myndigheter

Även nya samverkansformer mellan myndigheterna medför ett ökat informationsutbyte. Ett exempel på detta är möjligheten för Försäkringskassan och Arbetsförmedlingen att tillsammans med kommuner och landsting bilda s.k. samordningsförbund. Dessa förbund är egna myndigheter med uppgift att sköta den finansiella samordningen av rehabiliteringsinsatser som enskilda personer kan behöva från de olika inblandade myndigheterna. Det finns ett stort antal samordningsförbund i landet. Datainspektionen har i ett tillsynsärende granskat ett samordningsförbund och förelagt det att upphöra att behandla personuppgifter som inte är enbart av administrativ karaktär.[15] Beslutet motiverades i huvudsak med att samordningsförbundets uppdrag inte överensstämde med ändamålen för behandlingen av andra uppgifter än sådana som är enbart av administrativ karaktär. Datainspektionen hade inledningsvis konstaterat att förbundet var personuppgiftsansvarigt för ett it-system i vilket även känsliga uppgifter hanterades. Den personal som använde sig av it-systemet i sin dagliga verksamhet, s.k. koordinatorer, var inte är anställda hos samordningsförbundet, utan i huvudmännens egna, ordinarie verksamheter och ställdes till samordningsförbundets för-

[14] Regeringens proposition *Behandling av personuppgifter inom skatt, tull och exekution*, prop. 2000/01:33sid 142f.

[15] Datainspektionens beslut den 1 mars 2016 i dnr 391-2015.

fogande genom samverkansavtal. Huvudmän för förbundet var i ärendet Arbetsförmedlingen, Försäkringskassan, Region Östergötland och tre kommuner.

Utöver de exempel på ökad insamling, spridning och användning som redovisats här, bör ett belysande exempel från hälso- och sjukvården nämnas i detta sammanhang. I ett ärende hos Datainspektionen hade ett landsting givit direktåtkomst till uppgifter om landstingets samtliga patienter till en kommun, till ett annat landsting och till en privat vårdgivare, utan att först ha begränsat behörigheterna och utan att först ha informerat patienterna om spridningen på ett tillräckligt sätt.[16]

Skyddade personuppgifter

Myndigheterna hanterar i dag ett ökande antal skyddade personuppgifter i sina system. Skyddade personuppgifter är en samlingsrubrik som Skatteverket använder för de olika skyddsåtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter. Det är av stor vikt att dessa uppgifter hanteras på rätt sätt av alla inblandade myndigheter, eftersom ett röjande kan få mycket allvarliga konsekvenser för den enskilde. I slutet av september 2015 hade 14 503 personer sekretessmarkering eller kvarskrivning.[17] Motsvarande siffra för år 2014 var 13 109, och för år 2013 var siffran 12 153. Behovet av ett förstärkt skydd för hotade och förföljda personers personuppgifter har nyligen utretts av Trygghetsutredningen som i sitt slutbetänkande lämnat en rad förslag till åtgärder för att stärka skyddet.[18]

Den ökande komplexiteten i e-förvaltningen innebär särskilda risker för personer med skyddade personuppgifter. Ett belysande exempel på detta är att Stockholms läns landsting enligt egen bedömning inte förmår upprätthåll ett tillräckligt bra skydd i sina olika it-system. Efter en granskning år 2011 konstaterade landstingsrevisorerna att personer med skyddad identitet ”dessvärre inte kan besöka

[16] Datainspektionens beslut den 29 juni 2010 i dnr 1390-2009.

[17] Antalet personer som beviljas fingerade personuppgifter är mycket mindre, 2014 var det 8 personer och 2013 var det 11 personer vars ansökningar beviljades. Det är Polismyndigheten som beslutar om fingerade personuppgifter, medan Skatteverket beslutar om kvarskrivning och sekretessmarkering i folkbokföringsdatabasen.

[18] Trygghetsutredningens betänkande Ökad trygghet för hotade och förföljda personer, SOU 2015:69.

hälso- och sjukvården utan att riskera att få sina uppgifter röjda”.[19] Med anledning av rapporten beslutade hälso- och sjukvårdsnämnden i april 2016 att journaler för personer med skyddade personuppgifter ska kunna vara pappersbaserade ”för att uppnå maximalt personskydd”. Underlag för beslutet var, utöver den nämnda revisionsrapporten, ett tjänsteutlåtande från hälso- och sjukvårdsförvaltningen i vilket sägs att:

> …dagens journalsystem och andra elektroniska system och dess behörighetshantering är inte utformade så att det i tillräcklig omfattning begränsar informationsdelning och därmed spridning av patientinformation för patienter med skyddade personuppgifter. Finns information i ett elektroniskt journalsystem är dels skyddsförmågan i journalsystemet begränsad, dels överförs viss information per automatik till en mängd andra system inom vård och administration där möjligheten att upprätthålla informationsskyddet också är begränsat.[20]

11.1.3 Betydelsen av att fastställa personuppgiftsansvaret

På senare år har det vid några tillfällen uppstått frågor förknippade med frågan om vem som är personuppgiftsansvarig, både när det gäller behandling av personuppgifter i kommunikationen mellan enskilda och myndigheter och mellan olika myndigheter. Frågan är av stor betydelse för dataskyddet eftersom personuppgiftsansvaret innefattar ett ansvar att se till att personuppgifter hanteras bara om det är lagligt. Personuppgiftsansvaret innebär således ett ansvar att se till att det finns ett rättsligt stöd för behandlingen, men även ett ansvar för att informera enskilda om personuppgiftsbehandlingen och att vidta lämpliga säkerhetsåtgärder för att skydda personuppgifterna mot ändringar, otillåten spridning av eller otillåten tillgång till personuppgifterna och mot varje annat slag av otillåten behandling.

[19] Projektrapport 7/2011 *Skyddad identitet – hur hanteras personer med skyddad identitet inom vården?* Landstingsrevisorerna i Stockholms läns landsting. Skyddad identitet är i rapporten i huvudsak liktydigt med skyddade personuppgifter.

[20] Hälso- och sjukvårdsnämndens i Stockholms läns landsting beslut den 19 april 2016, samt tjänsteutlåtande den 26 februari 2016 från hälso- och sjukvårdsdirektören med dnr HSN 1112-1533.

Ett exempel på sådan oklarhet (som numera klarlagts) är Försäkringskassans tjänster för sms-anmälan av tillfällig föräldrapenning samt myndighetens s.k. infratjänst som används vid arbetsgivares anmälan av anställdas sjukdomsfall (den sistnämnda använder sig av SHS som nämns ovan). I båda fallen är det fråga om att uppgifter lämnas genom elektroniska kommunikationskanaler via olika operatörer. Uppgifterna är inte tillgängliga för Försäkringskassan förrän de når kassans elektroniska mottagningsställen. Efter en inspektion förelades Försäkringskassan av Datainspektionen att genomföra en risk- och sårbarhetsanalys av de aktuella tjänsterna. Försäkringskassan motsatte sig detta och menade att statliga myndigheter inte ska behöva lägga ned resurser på att analysera risker som hänför sig till sådant som de inte kan åtgärda. Frågan fick slutligen avgöras av Högsta förvaltningsdomstolen[21] som till att börja med konstaterade att Försäkringskassan saknar faktisk möjlighet att påverka hur uppgifterna hanteras innan de blir tillgängliga hos kassan, och att detta kan innebära svårigheter vid bedömningen av de skyldigheter och sanktionsmöjligheter som föreskrivs i personuppgiftslagen och som tar sikte på personuppgiftsansvaret. Enligt HFD hindrar detta emellertid inte att Försäkringskassan åläggs att redovisa säkerheten vid behandlingen av personuppgifter enligt 43 § b personuppgiftslagen. Detta gäller trots att en sådan redovisning möjligen kan komma att vara ofullständig i vissa hänseenden när det gäller säkerheten för personuppgifter hos operatörer eller avsändare.

Liknande frågeställningar har uppkommit i e-tjänsten Mina meddelanden, som är en tjänst för enskilda personer att kunna ta emot meddelanden digitalt från olika myndigheter. När e-tjänsten redan hade tagits i drift, vände sig Skatteverket till Datainspektionen för att få vägledning i frågan om personuppgiftsansvaret för hanteringen av personuppgifter i tjänsten.[22] Datainspektionen gjorde bedömningen att avsändande myndighet är ensamt personuppgiftsansvarig för behandling av uppgifterna i meddelandena – vilket innefattar ett personuppgiftsansvar gentemot de registrerade avseende säkerheten för uppgifterna – åtminstone till dess att meddelandena tillgängliggjorts för mottagaren. Brevlådeoperatörernas behandling av personuppgifterna görs under den tiden för avsändande myndighets räkning. Brevlådeoperatören har i egenskap av personuppgiftsbiträde

[21] HFD 2012 ref. 21.
[22] Datainspektionens beslut den 27 april 2015 i dnr 111-2014.

ett avtalsrättligt ansvar för säkerheten gentemot avsändande myndigheter, men brevlådeoperatören har inte ett personuppgiftsansvar enligt personuppgiftslagen gentemot de registrerade för uppgifterna i avsända meddelanden. Däremot är brevlådeoperatören personuppgiftsansvarig för behandlingen av de ytterligare personuppgifter som fordras för att meddelandena ska kunna tillgängliggöras i aktuell brevlåda och för behandlingen av kunduppgifter i sitt eget register.

Ett exempel på myndighetssamverkan som gör det svårt för den enskilde användaren att förstå vilken myndighet som han eller hon kommunicerar med och var uppgifterna till slut hamnar, är www.verksamt.se. Det är en webbplats där Bolagsverket, Skatteverket och Tillväxtverket tillsammans tillhandahåller e-tjänster och information till personer som vill starta företag.

11.1.4 Brister i beställarkompetens

E-delegationen har under flera års tid pekat på behovet av ökad kompetens hos myndigheterna när det gäller att beställa utveckling av e-förvaltningstjänster. Behovet omfattar kompetens att ställa krav i samband med exempelvis upphandlingar eller vid ingåendet av andra avtal, i frågor som gäller de tekniska och juridiska förutsättningarna för utvecklingen av e-förvaltningstjänster och som inbegriper integritetskyddet.

11.1.5 Potentiella handlingar och metadata

Begreppet handling i 2 kap. tryckfrihetsförordningen avser inte endast framställning i skrift eller bild – dvs. konventionella handlingar – utan också upptagningar som kan läsas, avlyssnas eller på annat sätt uppfattas med tekniskt hjälpmedel samt sammanställningar av sakligt sammanhängande uppgifter som en myndighet kan göra med hjälp av tillgängliga program, s.k. potentiella handlingar. En förutsättning för att även dessa ska anses som handlingar i tryckfrihetsförordningens mening, är att sammanställningen ska kunna göras med rutinbetonade åtgärder. Därmed avses att det ska vara fråga om en begränsad arbetsinsats och utan nämnvärda kostnader. Att en uppgiftssamling inte tidigare har existerat i sammanställd form hindrar däremot inte att en uppgiftssammanställning kan vara

att betrakta som allmän handling.[23] En arbetsinsats på 4–6 timmar går enligt Högsta förvaltningsdomstolens mening utöver vad som kan anses utgöra en begränsad arbetsinsats som inte är förknippad med några nämnvärda kostnader.[24]

En sammanställning av uppgifter ur en upptagning för automatiserad behandling anses dock enligt tryckfrihetsförordningen inte förvarad hos myndigheten, om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig. Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person.

Med tanke på de ökande tekniska möjligheterna att med begränsade arbetsinsatser sambearbeta uppgifter av olika format, t.ex. genom s.k. data mining, kan det i dag rimligen antas finnas långt fler potentiella handlingar hos myndigheterna än tidigare.

En relaterad företeelse är s.k. metadata hos myndigheterna. Metadata är data om data. Olika slags metadata behövs för att det överhuvudtaget ska vara möjligt att omvandla grunddatat till begriplig och användbar information. De flesta metadata är inte synliga för användaren, utan ligger inbäddade i de filer som innehåller dokument eller uppgifter. Digitala dokument är t.ex. försedda med information om filformat, författare, datum för färdigställande av dokumentet osv. På samma sätt som andra uppgifter hos myndigheten, kan metadata vara att betrakta som allmänna handlingar i tryckfrihetsförordningens bemärkelse.

Den enskilda person som vill kontakta en myndighet för att exempelvis framföra ett klagomål eller begära ut en allmän handling, använder sig i dag ofta av e-post eller ett digitalt formulär på myndighetens webbplats. Det innebär att den enskilde oftast efterlämnar någon form av uppgifter om sin identitet, såväl hos myndigheten i fråga, som hos sin e-postleverantör, internetleverantör och hos de företag som kontrollerar de servrar som e-postmeddelandet passerar på sin väg till myndigheten. Dessa kan även ta del av innehållet i e-postmeddelandet om det inte är skyddat genom exempelvis kryptering, som dock sällan används av privatpersoner. E-post och webb-

[23] JO:s ämbetsberättelse 2006/07 s. 478.
[24] HFD 2015 ref. 25.

formulär förenklar således kommunikationen med myndigheterna, men innebär också en exponering av både identitet och innehåll som många enskilda troligtvis inte är fullt medvetna om.

Uppgifter i allmänna handlingar, oavsett om det rör sig om uppgifter i själva dokumenten eller metadata, som finns hos myndigheter, är underställda arkivregelverket som har bevarande som huvudregel. Arkivförfattningarna har i dessa fall företräde framför personuppgiftslagen.

11.1.6 Offentlighetsprincipen

E-delegationen har påpekat att det finns brister i integritetsskyddet som följer av en tillämpning av offentlighetsprincipen. Som exempel nämner delegationen att handlingar med integritetskänsliga personuppgifter i dag lämnas ut i fysisk form, dvs. på papper, till kommersiella aktörer, med stöd av offentlighetsprincipen, varefter de skannas in och hanteras digitalt. Med utnyttjande av s.k. utgivningsbevis används sedan uppgifterna i en privat leverantörs kommersiella verksamhet där de kan lämnas ut automatiserat och till och med publiceras på internet. E-delegationen påpekar att detta, förutom att medföra ett eftersatt integritetsskydd, också påverkar enskildas tilltro till myndigheter. Enskilda personer ser hur uppgifter om dem själva, som de många gånger tvingats lämna ifrån sig, används i kommersiell verksamhet och förstår inte varför myndigheterna låter det ske.[25]

Ett konkret exempel på det ovan beskrivna förfarandet är Lantmäteriets massutlämnanden i pappersform av uppgifter ur lägenhetsregistret. Dessa uppgifter skannas sedan in och hanteras digitalt av företag som bl.a. kan publicera uppgifterna på nätet.

Den svenska offentlighetsprincipen och det europeiska dataskyddsregelverket kan sägas verka i olika riktningar på ett principiellt plan: offentlighetsprincipen har offentlighet som utgångspunkt (och sekretessbestämmelser som reglerar undantagen), medan dataskyddsdirektivets huvudregel är att personuppgifter inte får spridas (om inte spridningen har stöd i någon av direktivets bestämmelser).

[25] E-delegationens slutbetänkande *En förvaltning som håller ihop*, SOU 2015:66.

Förhållandet mellan den svenska offentlighetsprincipen och dataskyddsbestämmelserna har berörts både i förarbeten och i den juridiska doktrinen. En sammanfattning ges i *Personuppgiftslagen. En kommentar*:

> Offentlighetsprincipen enligt 2 kap. tryckfrihetsförordningen innefattar en rätt för varje svensk medborgare att hos myndigheter ta del av allmänna handlingar med personuppgifter i den utsträckning handlingarna inte innehåller uppgifter för vilka gäller sekretess. Den som begär att få ta del av allmänna handlingar har vidare i allmänhet rätt att få vara anonym. Offentlighetsprincipen innebär således i praktiken att myndigheterna är skyldiga att sprida en stor mängd personuppgifter till en obestämd krets av mottagare som kan utnyttja uppgifterna för ett okänt antal ändamål.[26]

I takt med digitaliseringen uppkommer nya utmaningar för offentlighetsprincipen. Ju bättre och billigare tekniska möjligheterna det finns att sambearbeta uppgifter med andra data och att sprida uppgifter med hjälp av nätet, desto större blir det kommersiella värdet av de personuppgifter som finns hos myndigheterna. Många företag vill därför få åtkomst till uppgifterna. En del myndigheter kan ta betalt för vissa utlämnanden. Uppgifterna får därmed en ekonomisk betydelse även för myndigheterna. När företag har fått ut uppgifter med stöd av offentlighetsprincipen, kan de sprida och hantera uppgifterna för helt andra ändamål än dem för vilka myndigheten ursprungligen samlade in uppgifterna. Ibland kan företagen även publicera integritetskänsliga uppgifter på nätet med grundlagsskydd genom s.k. frivilliga utgivningsbevis, och därmed undkomma det integritetsskyddande regelverket. Frågan om de frivilliga utgivningsbevisens innebörd för den personliga integriteten, är för närvarande föremål för utredning i Mediegrundlagskommittén.[27]

11.1.7 PSI-lagstiftningen

Genom det s.k. PSI-direktivet (Public Sector Information) från år 2003 fastställdes regler om hur enskilda och företag kan använda handlingar från den offentliga sektorn för andra ändamål än vad de

[26] Öman & Lindblom, *Personuppgiftslagen. En kommentar*, 15 oktober 2015, Zeteo, kommentaren till 8 § andra stycket personuppgiftslagen.
[27] Ju 2014:17.

ursprungligen avsågs för. Sådan användning benämns i direktivet som vidareutnyttjande. I juni 2013 antogs ett ändringsdirektiv till det ursprungliga PSI-direktivet.[28]

PSI-direktivet har genomförts i svensk rätt genom lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen (ibland kallad PSI-lagen). Syftet med lagen är att främja utvecklingen av en informationsmarknad genom att underlätta enskildas användning av handlingar som tillhandahålls av myndigheter. Lagen innehåller bestämmelser som avser att förhindra att myndigheter beslutar om sådana villkor för hur handlingar får användas som begränsar konkurrensen.

Eftersom PSI-lagen syftar till att öka spridningen och vidareutnyttjande av uppgifter, även personuppgifter, har den betydelse för enskildas personliga integritet.

PSI-utredningen resonerade på följande sätt beträffande regelverkets innebörd för den personliga integriteteten:

> Vid elektroniskt utlämnande ska myndigheterna tillämpa bestämmelser i flera, delvis samverkande, regelverk. De är komplicerade och innefattar flera svåra bedömningar. Reglernas utformning och förhållande till varandra kan medföra risk för felaktiga bedömningar av vad som får och vad ska lämnas ut elektroniskt. Förutom risken för att personuppgifter kan komma att lämnas ut för vidareutnyttjande i strid med gällande bestämmelser, medför de komplicerade regelverken även att fördelarna med vidareutnyttjandet begränsas.[29]

I betänkandet konstaterade PSI-utredningen sammanfattningsvis att insatserna för att öka spridningen av information från myndigheter till resten av samhället, i kombination med en svårtillämpad och delvis oklar lagstiftning, medför att det finns påtagliga risker för att det leder till fler fall av felaktig spridning av information och otillbörliga intrång i den personliga integriteten.

[28] Betänkande från PSI-utredningen, *Ett steg vidare – nya regler och åtgärder för att främja vidareutnyttjande av handlingar*, SOU 2014:10.
[29] SOU 2014:10.

11.1.8 Eget utrymme

På senare år har flera myndigheter utvecklat digitala lagringsplatser som kan användas av enskilda i deras kontakter med myndigheten eller i ärenden som på något sätt berör myndigheten. Dessa lagringsplatser har kommit att kallas för ”egna utrymmen”. Ett exempel på sådan plats är Arbetsförmedlingens CV-databas som även omnämns nedan.

Med eget utrymme menas enligt E-delegationen[30] ett skyddat förvar som tillhandahålls elektroniskt endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Det rör sig om ”en elektronisk miljö som myndigheten tillhandahåller, ett eget utrymme där endast den nyttoinformation finns som användaren ska få ta del av”. Enligt de tolkningar som E-delegationens vägledning utgår från är myndigheten inte ansvarig för nyttoinformationen i ett eget utrymme. Nyttoinformation i användares eget utrymme finns enligt E-delegationen inte i någon ingiven handling enligt förvaltningslagen. Detta material utgör enligt E-delegationens uppfattning inte heller allmänna handlingar.

Det kan i sammanhanget noteras att Myndigheten för samhällsskydd och beredskap inte delar E-delegationens bedömning att material i de s.k. egna utrymmena inte kan utgöra allmänna handlingar. Myndigheten anser att E-delegationen inte på ett övertygande sätt visat att den föreslagna tolkningen av undantagsregeln i tryckfrihetsförordningen är så rättsligt hållbar att den kan läggas till grund för ett omfattande och resurskrävande utvecklingsarbete på e-förvaltningsområdet.[31]

Det kan noteras att inte heller Datainspektionen delar E-delegationens bedömning avseende personuppgiftsansvaret i egna utrymmen. Enligt Datainspektionen regleras personuppgiftsansvaret antingen i registerförfattningar eller bestäms utifrån vem som bestämmer ändamål och medel med behandlingen enligt 3 § personuppgiftslagen. Det leder normalt till att myndigheter har personuppgiftsansvar för personuppgifter i egna utrymmen, dvs. även för det som benämns nyttoinformation.[32]

---

[30] E-delegationens publikation *Juridisk vägledning för verksamhetsutveckling inom e-förvaltning*, version 2.0 den 19 mars 2015.

[31] MSB:s remissvar 14 oktober 2014 avseende SOU 2014:39, myndighetens dnr 2014-3403-2.

[32] Fotnot 6 i *Juridisk vägledning för verksamhetsutveckling inom e-förvaltning*, version 2.0 den 19 mars 2015.

I ett mål om rätten att ta del av allmän handling, har Kammarrätten i Stockholm ansett att vissa handlingar i ett s.k. eget utrymme hos Arbetsförmedlingen får anses förvarade hos myndigheten endast som ett led i teknisk bearbetning eller teknisk lagring för annans räkning.[33] Handlingarna är därmed inte allmänna. Målet rörde handlingar i Arbetsförmedlingens CV-databas. CV-databasen består av konton för arbetssökande och arbetsgivare. Arbetssökande kan lagra CV:n och annan information i ett utrymme kallat för ”Min profil” och arbetsgivare kan söka bland profilerna, läsa dem och skicka förfrågningar. Databasen är inte något verksamhetssystem hos Arbetsförmedlingen och myndighetens handläggare saknar åtkomst till systemet.

Det kan förekomma att företag uppmanar enskilda personer att använda sig av sin åtkomst via e-legitimationen till den enskildes egna uppgifter hos en myndighet, så att företaget på distans kan genomföra ändringar i den enskildes val och inställningar som gynnar företaget i fråga. Det har inträffat beträffande fondval som kan göras hos Pensionsmyndigheten (som i och för sig inte görs i ett s.k. eget utrymme).[34]

11.1.9 Medborgarprofilering[35]

Det finns myndigheter som arbetar med att skapa profiler över personer som har ärenden hos dem, i syfte att kunna arbeta med smarta kontroller. I texten som följer kommer vi att använda begreppet kund, när den myndighet som det är frågan om själv använder det begreppet.

En myndighet som arbetar med profiler är Försäkringskassan. Arbetet är en del i utförandet av regeringens instruktioner i myndighetens regleringsbrev de senaste åren och beskrivs i en rapport från Försäkringskassan.[36]

---

[33] Kammarrättens i Stockholm dom den 26 oktober 2015 i mål nr 7369-15, som vunnit laga kraft.

[34] Se varning publicerad den 31 december 2015 på www.pensionsmyndigheten.se med rubriken *Logga inte in åt någon annan*, samt artikeln *Myndigheten varnar för pensionsbluffen*, publicerad på www.expressen.se den 6 januari 2016, författad av Therese Färsjö.

[35] När det gäller både medborgarprofilering och kontroller på nätet, har Integritetskommittén haft kontakter och möten med de två berörda myndigheterna, Skatteverket och Försäkringskassan., för att få information om vad de gör.

[36] Försäkringskassans beslut den 21 februari 2014, dnr 3421-2014.

I rapporten hänvisar Försäkringskassan till hur framgångsrika företag och myndigheter agerar i sina analyser av kunddata. När andra aktörer analyserar sina data för att exempelvis bedöma vilken kreditrisk det skulle innebära att låna ut pengar till en potentiell kund, eller hur sannolikt det är att en kund kommer att tacka ja till ett riktat köperbjudande, så handlar det för Försäkringskassan om att analysera sin information för att bedöma kundernas behov samt risker för felaktiga beslut och systematiskt utnyttjande av socialförsäkringen. Som en del i detta arbete utvecklar Försäkringskassan analytiska modeller och urvalsprofiler.

En urvalsprofil hos Försäkringskassan kan vara olika komplex i form av metod (enkla logiska villkor – komplexa statistiska modeller) och mängden information som den bygger på (en uppgift i aktuellt ärende – sammanvägning av indikatorer från aktuellt ärende, kundens socialförsäkringshistorik samt information om kundens nätverk, såsom assistansbolagets samlade verksamhet).

Den metodik som enligt Försäkringskassans bedömning har störst potential att använda myndighetens information och ackumulerade kunskap på ett träffsäkert sätt är s.k. prediktiv analys. Försäkringskassan beräknar potentiella riskindikatorer eller prediktorer som beskriver exempelvis innehållet i ansökningen och kundens historiska ersättningsmönster och kombinerar dessa med data från utfallet av de kontrollerade ansökningarna. Sedan används statistisk modellering och data mining-algoritmer för att systematiskt testa vilka av de potentiella riskindikatorerna som tillsammans bäst kan särskilja ärenden med hög risk från ärenden med låg risk. De prediktiva modellerna används sedan för att göra förutsägelser om framtiden eller andra okända händelser, exempelvis för att uppskatta sannolikheten för fel i nya ansökningar.

Försäkringskassan skriver i rapporten också att den nya lagstiftning inom personlig assistans, som trädde i kraft år 2013, bl.a. har gett Försäkringskassan möjligheter att utöka informationsutbytet med andra myndigheter. Myndigheten kan därmed mer effektivt förebygga och upptäcka felaktiga utbetalningar och bidragsbrott inom området. Det finns enligt Försäkringskassan sannolikt också stor potential med ett vidareutvecklat informationsutbyte vad gäller exempelvis information om företag som är verksamma inom välfärdssektorn.

I sin rapport beskriver Försäkringskassan också det kontrollarbete som utförs efter tips från allmänheten. I rapporten benämns detta som impulser från allmänheten. Försäkringskassan vill i framtiden på ett mer systematiskt sätt analysera innehållet i impulserna. Exempelvis skulle Försäkringskassan utifrån data och kunskap som finns inom myndigheten i framtiden kunna skapa en mer effektiv prioritering bland dessa och fokusera på ”rätt” impulser.

I Försäkringskassans rapport nämns vidare att det i dag finns ett relativt väl utbyggt elektroniskt informationsutbyte mellan Försäkringskassan och andra myndigheter, såsom Skatteverket, Arbetslöshetskassorna och Centrala studiestödsnämnden. Det finns enligt Försäkringskassan en ambition att ytterligare stärka arbetet med elektroniskt informationsutbyte med andra myndigheter och organisationer

I Försäkringskassans rapport förs inga resonemang om eventuella risker för den personliga integriteten eller för diskriminering av vissa kunder, som myndighetens kontrollarbete kan medföra. Det resoneras heller inte om hur den för myndigheten tillämpliga registerförfattningen förhåller sig till kontrollarbetet. Försäkringskassan har till Integritetskommittén uppgett att myndigheten har påpekat för regeringen att det behövs ett förtydligande av 114 kap. socialförsäkringsbalken för att regelverket tydligt ska stödja dagens arbetssätt med kontroller. Försäkringskassan anser dock att nuvarande lagstiftning ger stöd för arbetssättet. Försäkringskassan uppger också att myndigheten inte specifikt informerar enskilda och allmänheten om vilka kontroller som görs. Skälen för detta uppger Försäkringskassan vara att det skulle försvåra arbetet och att det inte finns någon skyldighet att lämna sådan information.

Hos Skatteverket utförs ett liknande arbete för att förebygga felaktigheter, vilket bl.a. framgår av myndighetens rapport *Framtidens kontroll*.[37] I rapporten sägs bl.a. att ”det traditionella sättet att med hjälp av stora datamängder och med hjälp av olika typer av algoritmer hitta misstänkta fel behöver förstås fortsätta finnas och även fortsätta utvecklas”. På ett annat ställe i rapporten anges att Skatteverket gör s.k. nätverksanalyser där skattebetalarnas nätverk undersöks. Det finns dock ingen närmare beskrivning av Skatteverkets hantering av personuppgifter för dessa ändamål i rapporten. I rapporten

[37] Skatteverkets rapport *Framtidens kontroll*, publicerad 11 november 2015.

nämns att de enskildas rätt till personliga integritet måste beaktas. Avslutningsvis anförs i rapporten att Skatteverket tydligt bör slå fast att urvalen aldrig använder de diskrimineringsgrunder som är uppräknade i 1 kap. 2 § regeringsformen. Rapporten innehåller ingen analys av hur den för myndigheten tillämpliga registerförfattningen förhåller sig till kontrollarbetet – dess syfte är snarare att på ett övergripande plan diskutera vilka kontrollåtgärder som är lämpliga och rimliga även ur de kontrollerade personernas synvinkel.

Skatteverket har till Integritetskommittén uppgett att myndigheten anser att det nuvarande författningsstödet inte ger verket någon möjlighet att i förväg, innan det finns ett ärende, upprätta riskprofiler för enskilda (fysiska) personer. Skatteverket efterlyser därför en reglering som redogör för vad som gäller för närvarande och som ger en utökad möjlighet att göra riskbedömningar med hög träffsäkerhet i urval och därmed stödjer hur man arbetar i dag och vill kunna arbeta i framtiden. Skatteverket uppger också att myndigheten inte informerar de berörda om arbetet med riskbedömningar, och inte heller om uppgiftsinhämtningen på nätet, på sociala medier eller om det som görs med Skatteverkets s.k. spindlar (se följande avsnitt). Informationen ges istället samband med att ett eventuellt ärende öppnas.

11.1.10 Kontroller på nätet

Skatteverket är en myndighet som kommit långt i användningen av webbrobotar i sin kontrollverksamhet på nätet. Webbrobotorna kallas ibland även för spindlar. När det gäller Skatteverket handlar det om en programvara som konstruerats för att automatiskt söka efter ekonomisk aktivitet på nätet, som ger intäkter som inte tagits upp till beskattning. Verksamheten startades år 2007 och bedrivs med program som går under beteckningarna EC Eyes, Xenon och Data Detective. Kontroller med spindelhjälp inriktas på webbplatser där handel och annan ekonomisk verksamhet bedrivs. Exempelvis har säljare hos Tradera, Blocket och Ebay granskats, men även webbplatser för pokerspel. Redan år 2007 hittade Skatteverket med spind-

larnas hjälp oredovisade intäkter på 420 miljoner kronor.[38] Enligt uppgift från Skatteverket till Integritetskommittén i december 2015 pågår verksamheten alltjämt på samma sätt.

Förutom att låta specialtillverkade program söka av nätet, använder sig vissa myndigheter även av enklare, manuella sökningar på nätet för att inhämta underlag för beslut som rör enskilda personer. Företeelsen har granskats av Riksdagens ombudsman (Justitieombudsmannen), bl.a. i ett ärende där en socialsekreterare som utredde en ansökan om försörjningsstöd, hämtade viss information om de sökande från deras Facebooksidor och från en annan persons blogg.[39] Den information det var frågan om i ärendet var tillgänglig för alla med konto på Facebook. I beslutet kom Justitieombudsmannen fram till att det inte finns några formella hinder mot att socialtjänsten inom ramen för en utredning om försörjningsstöd hämtar in offentliga, dvs. allmänt tillgängliga, uppgifter om biståndssökanden från internet, vilket det bedömdes vara frågan om i ärendet. Justitieombudsmannen såg heller inga formella hinder mot att detta görs utan sökandens samtycke. Även om det inte krävs något samtycke bör dock socialtjänsten enligt Justitieombudsmannen informera om att man kan komma att hämta in eller kontrollera uppgifter på t.ex. internet.

Justitieombudsmannen sammanfattar i en övergripande redovisning av iakttagelser året 2014/2015, att frågor om informationsinhämtning från internet och handläggares och myndigheters användning av sociala medier var företeelser som tidigare inte hade förekommit i Justitieombudsmannens klagomålsärenden. Det är därför angeläget att frågan om dessa nya verktyg i myndigheternas verksamhet kommer upp till diskussion hos berörda myndigheter. I den diskussionen är skyldigheten att iaktta saklighet och opartiskhet i verksamheten central. Enligt Justitieombudsmannen kan man förvänta sig fler påståenden och anmälningar om jäv. Risken är stor att allmänhetens förtroende för myndigheterna påverkas, även om en granskning skulle mynna ut i att det inte bedöms vara fråga om jäv. Justitieombudsmannen framhåller att det är angeläget att myndighe-

[38] Tomas Carlsson, *Skattespindlar hittar miljoner*, publicerad den 29 oktober 2008 på www.nyteknik.se.

[39] JO:s beslut den 15 januari 2015 i ärendet med dnr 2611-2013.

terna tar fram riktlinjer och handläggningsrutiner om man avser att använda sig av sociala medier och informationssökning på internet i verksamheten.[40]

Vissa myndigheter har sådana riktlinjer för efterforskningsåtgärder på nätet. Ett exempel på detta är Skatteverkets riktlinjer.[41] Enligt dessa riktlinjer är det inte bara en möjlighet för Skatteverket att använda öppna sidor på internet och i sociala medier vid efterforskning, det kan även ses som en skyldighet för myndigheten att använda sådan information som är allmänt tillgänglig. Efterforskning kan enligt riktlinjerna göras på s.k. öppna sidor. Det innebär enligt riktlinjerna att sidor på internet som kräver inloggning utan någon egentlig motprestation omfattas. Skälet för inloggning kan vara att man vill undvika spam eller kunna stänga av en användare som skriver olämpliga saker. Enligt riktlinjerna kan dessa sidor således användas för efterforskning. Men en annan bedömning görs i riktlinjerna när det gäller sidor som användaren valt att inte göra allmänt tillgängliga och som kräver medlemskap, en inbjudan, att man är vän med en person eller på något annat sätt förtrolig eller som ställer krav på en personlig lösen. Dessa bedöms ingå i vad som kallas för den privata sfären inom vilken efterforskning inte får göras.

11.1.11 E-legitimation som avslöjar användaren

E-legitimationer används ofta för att säkerställa en säker kommunikation mellan myndigheterna och enskilda personer i olika e-tjänster.

E-legitimationerna utges av vissa banker, dvs. av företag. När en enskild person använder sig av sin e-legitimation för att kommunicera med en myndighet, exempelvis en offentlig vårdgivare eller Kronofogdemyndigheten, kan det företag som utgivit legitimationen ta del av information om t.ex. vilken myndighet den enskilde kontaktar, när på dygnet detta görs och från vilken plats. Innehållet i kommunikationen med myndigheten kan företaget däremot inte ta del av. Den information som företaget kan ta del av kan komma till nytta i kontroller av säkerheten i kommunikationen, men kan även

[40] JO Lilian Wiklunds övergripande redovisning av iakttagelser under året 2014/15, publicerad på www.jo.se, daterad den 30 november 2015.
[41] Riktlinjer beslutade den 21 september 2014, dnr 131 530342-14/111.

utnyttjas för andra ändamål. Sanktioner mot användning för andra ändamål än för att kontrollera säkerheten, regleras i dag i avtal mellan företagen och myndigheterna.

11.1.12 Myndigheter med uppgifter i molnet

Det blir allt vanligare att myndigheter använder sig av molntjänster för att hantera olika slags information, bl.a. uppgifter om anställda eller andra enskilda personer. Den mesta informationen som läggs ut i molnet är dock inte personuppgifter. Skolor är ett exempel på sådana myndigheter. De kan hantera uppgifter om både eleverna och lärarna i molnet.

Kommittén behandlar molntjänster i skolan och molntjänster som egen företeelse i kapitel 7 respektive i kapitel 21.

Här kan däremot nämnas några exempel på molntjänster som används av andra myndigheter än skolor. I Integritetskommitténs kontakter med myndigheter har det framkommit att molntjänsten *Projectplace* används. Det är en tjänst för projektarbete som kan användas såväl för samarbeten inom en myndighet som för samarbeten mellan olika myndigheter (tjänsten används även i verksamheter utanför myndighetsvärlden).

En annan molntjänst som används av myndigheter är *Relation Desk* som är en tjänst för att få överblick och kontroll över flöden på myndighetens konton i sociala medier. Syftet med tjänsten är bl.a. att snabbare kunna svara på frågor och få veta vad som sägs på det sociala mediet, och att ta fram statistik över trafiken på myndighetens konto.

Molntjänsten *Barium* förekommer också hos myndigheter. I det exempel som vi har fått kännedom om, används tjänsten för att inom myndigheten hantera förbättringsförslag från de anställda.

11.1.13 Myndigheter i sociala medier och med gilla-knappar på webben

Allt fler myndigheter använder sig av sociala medier, som exempelvis Facebook, Instagram, Youtube, Linkedin, Google Plus, Flickr, Pinterest, Twitter, bloggar och diskussionsforum. Vanligt är att myndigheter skaffar egna konton i det sociala mediet för att kunna

informera allmänheten om sin verksamhet. Det har inte kommit till Integritetskommitténs kännedom att myndigheter även använder sig av sociala medier för intern kommunikation med de anställda, men det är långt ifrån otänkbart att det förekommer. Det finns sociala medier som konstruerats särskilt för organisationers interna kommunikation, exempelvis *Facebook at Work*, som nämns i kapitel 8 om arbetslivet.

Om myndigheten har ett eget konto, kan det innebära att personuppgifter behandlas i det sociala mediet. Den hanteringen anses myndigheten vara ansvarig för, och inte det sociala mediet. Det innebär att myndigheterna måste se till att följa reglerna i personuppgiftslagen och, i vissa fall, särskild registerlagstiftning.

Datainspektionen har publicerat ett informationsblad[42] om myndigheters, företags och andra organisationers ansvar för personuppgifter i sociala medier. Där ges vägledning beträffande vad en myndighet bör tänka på när myndigheten är aktiv på sociala medier.

E-delegationen har också tagit fram en vägledning med titeln *Myndigheters användning av sociala medier*.[43]

Det förekommer även att myndigheter sprider uppgifter om enskilda till sociala medier på andra sätt, troligen utan att helt förstå konsekvenserna. Myndigheter har t.ex. på sina webbsidor så kallade gilla-knappar till olika sociala medier. Knapparna kallas även för sociala insticksprogram eller plug-ins. Deras förekomst på myndigheternas webbsidor innebär att det sociala mediet kan få vetskap om vilken enskild person som besökt den aktuella myndighetens webbsida – även om besökaren inte klickar på knappen och även om besökaren inte har ett konto hos det sociala mediet i fråga. Den bakomliggande tekniken berörs i kapitel 13 om sociala medier och e-post och i kapitel 12 om konsumentområdet.

Företeelsen uppmärksammades under hösten 2015 av Dagens Nyheter som då beskrev några exempel på hur detta går till i praktiken.[44]

I artikeln nämns att ett amerikanskt företag loggar besök på ett landstings webbplats. Företaget arbetar med att förmedla sociala mediers gilla-knappar till sina kunder, som exempelvis kan vara

[42] Daterat maj 2014.
[43] Version 1.0, 2010-12-30.
[44] Linus Larsson och Kristoffer Örstadius, *Svenska myndigheter lämnar ut dina surfvanor*, publicerad den 2 september 2015 på www.dn.se.

svenska myndigheter. Företaget får genom besöket på webbsidan tillgång till uppgifter som exempelvis den enskilde besökarens ip-nummer, information om webbläsaren och från vilket land besöket görs. När Dagens Nyheter närmare granskade nätverkstrafiken mellan landstinget webbplats och det amerikanska företaget framgick att det som överförs innefattar information om vad besökaren på webbplatsen läser om i form av en rad nyckelord. Exempel på förekommande nyckelorden som kunde skickas var ”homosexualitet”, ”klamydia” och ”aids”. Nyckelorden tillsammans med ett unikt id-nummer gör att företaget kan följa besökaren på många andra webbplatser.

11.1.14 Informationssäkerhet

I Riksrevisionens granskning av informationssäkerheten i den civila statsförvaltningen[45] framkom att det finns omfattande brister i regeringens och myndigheternas arbete med informationssäkerhet. Riksrevisionens granskning visar att regeringen saknar en samlad bild av läget för informationssäkerheten i statsförvaltningen och därmed saknar möjligheten att styra effektivt. Inte heller stödmyndigheterna; Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, och Säkerhetspolisen har en samlad bild. Det råder en osäkerhet om hur starkt skyddet är, vilka händelser som har ägt rum och hur hoten utvecklas. Det är därför svårt att värdera riskerna och veta hur omfattande skyddet behöver vara. Riksrevisionens granskning visar att det finns brister inom flera områden, till exempel kompetens, upphandling, tillsyn, uppföljning samt styrning och samordning. Så mycket som 38 procent av myndigheterna bedömer till exempel att kompetens, mandat eller resurser inte räcker.

Under år 2014 genomförde Myndigheten för samhällsskydd och beredskap en kartläggning (genom en enkätundersökning) av hur statliga myndigheter tillämpar myndighetens föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10) och av hur

[45] RiR 2014:23.

myndigheterna i övrigt arbetar med informationssäkerhet.[46] Rapporten ger en god överblick över situationen hos de statliga myndigheter som besvarat enkäten.

Myndigheten för samhällsskydd och beredskap har under år 2015 genomfört en motsvarande granskning av informationssäkerheten hos kommuner och landsting.[47] Resultatet gav bl.a. vid handen att majoriteten av de kommuner som svarat på enkäten inte arbetar systematiskt med informationssäkerhet och att de heller inte kontrollerar följsamheten vad gäller informationssäkerhet.

Myndighetens för samhällsskydd och beredskap har uttryckt en viss oro för den hur e-förvaltningen utvecklas. Myndigheten skriver i remissvar på ett av E-delegationens betänkanden att myndigheten ”ser positivt på en utveckling av effektiv, säker och långsiktigt hållbar e-förvaltning. En sådan utveckling måste dock vila på en solid rättslig grund samt använda sig av lösningar som uppfyller krav på integritetsskydd och informationssäkerhet. En utveckling som inte på ett tillräckligt sätt har beaktat detta riskerar att, till och med på kort varsel, behöva stängas ned eller förändras i grunden i det fall den rättsliga grunden eller de säkerhetsmässiga förutsättningarna befinns otillräckliga. Konsekvenserna, både avseende ekonomiska förluster och förlorat förtroende hos allmänheten och näringslivet, kan bli avsevärda.”[48]

Utredningen NISU 2014 hade i uppdrag att föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system. Utredningen skulle även föreslå övergripande mål för samhällets informationssäkerhetsarbete samt ge förslag på hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur. I sitt slutbetänkande[49] konstaterar NISU 2014 bl.a. att behoven på informations- och cybersäkerhetens område är så omfattande i Sverige, att det inte behövs en, utan flera strategier. Utredningen föreslår därför en första strategi för statens

[46] Se rapporten *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*.

[47] Se rapporten *En bild av kommunernas informationssäkerhetsarbete 2015*, MSB, december 2015.

[48] MSB:s remissvar 14 oktober 2014 avseende SOU 2014:39, myndighetens dnr 2014-3403-2.

[49] Betänkande av NISU 2014, *Informations- och cybersäkerhet i Sverige, Strategi och åtgärder för säker information i staten*, SOU 2015:23.

informations- och cybersäkerhet för att åtgärda de mest angelägna bristerna i statsförvaltningen. Den föreslagna strategin uppställer sex mål för staten under regeringens ledning:

1. Staten förstärker styrning och tillsyn av informationssäkerheten i staten,
2. Staten blir en tydlig kravställare,
3. Staten kommunicerar säkert,
4. De statliga myndigheterna ska rapportera it-incidenter,
5. Statens förebyggande och bekämpande av it-relaterad brottslighet stärks och
6. Sverige ska vara och uppfattas som en stark internationell partner.

Myndigheten för samhällsskydd och beredskap har tagit fram vägledningar och praktiskt stöd för långsiktigt och systematiskt arbete med informationssäkerhet. Dessa finns samlade på webbplatsen www.informationssäkerhet.se.

11.1.15 Regeringens mål i lagmotiv, digital agenda och e-förvaltningsstrategi

I sin rapport *Informationssäkerheten i den civila statsförvaltningen*[50] beskriver Riksrevisionen utvecklingen genom att göra några nedslag i förarbeten från 1999 och framåt. År 1999 uttryckte regeringen att inriktningen för statsförvaltningen bör vara att all den information individer och företag behöver få från, och lämna till, myndigheter bör finnas tillgänglig elektroniskt.[51] År 2004 stegrades målsättningen genom att målet för varje myndighet ska vara att all information och service som med bibehållen eller ökad effektivitet, såväl ekonomisk som organisatorisk, kan tillhandahållas elektroniskt också ska tillhandahållas så.[52] I propositionen om behandling av personuppgifter inom studiestödsområdet år 2008 uttalar regeringen att den tekniska infrastrukturen för den offentliga förvaltningens kommunikation

[50] RiR 2014:23.
[51] Regeringens proposition *Ett informationssamhälle för alla*, prop. 1999/2000:86.
[52] Regeringens proposition *Från IT-politik för samhället till politik för IT-samhället*, prop. 2004/05:175.

med medborgarna bör bygga på internet.[53] I den förvaltningspolitiska propositionen år 2010 konstaterades slutligen att det finns en stor effektiviseringspotential att ta till vara med hjälp av tekniken och den ska också bidra till att förstärka förvaltningens öppenhet.[54]

Den 29 september 2011 beslutade regeringen om en ny strategi för it-politiken, *It i människans tjänst – en digital agenda för* Sverige[55], kallad den digitala agendan för Sverige. Enligt denna är målet för it-politiken att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.

I december 2012 presenterade regeringen sin e-förvaltningsstrategi *Med medborgaren i centrum*.[56] Strategin förtydligar och preciserar de mål och strategiska ställningstaganden som uttrycks i den förvaltningspolitiska propositionen[57] och i den digitala agendan för Sverige. I strategin sägs bl.a. att:

> …statsförvaltningen spelar en central roll i utvecklingen av Sverige. Den ska vara innovativ, samverkande, rättssäker och effektiv, samt ha en väl utvecklad kvalitet, service och tillgänglighet. Därigenom ska den bidra till Sveriges utveckling och ett effektivt EU-arbete. Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.

11.1.16 Samordning och styrning av utvecklingen

I mars 2014 rapporterade Statskontoret sitt regeringsuppdrag att utvärdera E-delegationen.[58] Statskontoret konstaterade att regeringen behöver stärka den samlade beslutsförmågan och genomförandekraften inom e-förvaltningsområdet.

Regeringen annonserade i budgetpropositionen för år 2015 en satsning under fyra år för att förstärka styrning och samordning av övergripande it-användning i statsförvaltningen. Regeringen vill se en ökad samordning och utveckling av informationsutbytet mellan myndigheter.

---

[53] Regeringens proposition *Behandling av personuppgifter inom studiestödsområdet*, prop. 2008/09:96.
[54] Regeringens proposition *Offentlig förvaltning för demokrati, delaktighet och tillväxt*, prop. 2009/10:175.
[55] Dnr N2011/342/ITP.
[56] Dnr N2012/6402/ITP.
[57] Prop. 2009/10:175.
[58] Dnr N2014/1630/ITP.

På Näringsdepartementet har det som ett led i satsningen inrättats en särskild e-förvaltningsenhet.

Regeringen har vidare uppdragit åt Ekonomistyrningsverket att ge stöd till regeringen och Regeringskansliet i samband med satsningen på e-förvaltning under åren 2015–2018.[59] Vidare ska Ekonomistyrningsverket inom ramen för satsningen ge stöd till de statliga myndigheterna.

E-delegationen avslutade sitt arbete den 30 juni 2015. I slutbetänkandet[60] sammanfattar E-delegationen dagsläget för e-förvaltningen med följande ord:

> Oavsett vilka vägval som görs i den offentliga sektorn behöver samverkan mobiliseras. För detta krävs centrala inriktningsbeslut och en nationell styrning och samordning.I dag finns även det s.k. E-samverkansprogrammet (eSam) som är en frivillig sammanslutning av berörda myndigheter med ett kansli placerat på Pensionsmyndigheten. I eSam ingår i dagsläget ingen myndighet som har i uppdrag att peka på möjliga problem för integritetsskyddet i e-förvaltningen, som exempelvis Datainspektionen eller Myndigheten för samhällsskydd och beredskap.

När det gäller samordning av e-förvaltningsutveckling för kommuner och landsting görs arbetet inom Sveriges Kommuner och Landsting där det koordineras i programkontoret Center för eSamhället (CeSam).

Regeringen har i oktober 2015 undertecknat en avsiktsförklaring tillsammans med Sveriges Kommuner och Landsting. Syftet med avsiktsförklaringen är att tydliggöra hur parterna kan stärka förutsättningarna för digital samverkan mellan stat, kommuner och landsting genom att peka ut ett antal områden för fördjupat samarbete. Dessa områden är främjande av digitala tjänster som förstahandsval, utveckling av förvaltningsgemensamma lösningar, underlätta samverkan kring gemensamma tjänster och infrastruktur samt samarbeta om initiativ för öppen innovation. Därtill syftar avsiktsförklaringen till att öka förutsättningarna för en stärkt styrning och uppföljning av digitaliseringen av det offentliga Sverige, samt verka

[59] Dnr N2015/03210/EF.
[60] SOU 2015:66.

för ett gemensamt budskap. I avsiktsförklaringen sägs att arbetet ska drivas utifrån ett antal grundläggande principer, bl.a. den enskildes rätt till sekretess och integritetsskydd.[61]

Regeringen har i oktober 2015 även tillsatt ett särskilt råd för digitaliseringen av det offentliga Sverige. Tanken är bl.a. att det i rådet ska lyftas strategiska frågor för att identifiera och diskutera utmaningar under genomförandet av regeringens satsning på e-förvaltning och vid behov föreslå åtgärder. Liksom i eSam ingår här ingen myndighet som har i uppdrag att peka på möjliga problem för integritetsskyddet i e-förvaltningen.

Riksrevisionen har en pågående granskning av digitaliseringen av den offentliga förvaltningen. Resultatet av granskningen kommer att presenteras i en rapport med planerad publicering i juni 2016. Riksrevisionen motiverar granskningen med att det sedan år 2000 har gjorts flera analyser som pekar på problem och oklarheter rörande förvaltningens förutsättningar för att utveckla e-förvaltning, framför allt förvaltningsgemensamma digitala tjänster. Regeringen har också tillsatt flera utredningar, råd och andra organ för att styra den svenska e-förvaltningen. Trots det har enligt Riksrevisionen problem och oklarheter inte hanterats fullt ut och regeringens styrning av den svenska e-förvaltningen har upplevts som fragmentarisk och kortsiktig.

11.2 Det skyddande regelverket

Hanteringen av personuppgifter inom e-förvaltningen regleras i ett stort antal olika författningar, beroende på inom vilket område av förvaltningen det handlar om. Exempelvis omfattas hanteringen av personuppgifter inom socialförsäkringsområdet av 114 kap. i socialförsäkringsbalken, inom skatteområdet av bl.a. lagen (2001:181) om behandling av personuppgifter i Skatteverkets beskattningsverksamhet, inom hälso- och sjukvården av patientdatalagen (2008:355) och inom socialförvaltningen av lagen (2001:454) om behandling av personuppgifter inom socialtjänsten. För vissa områden, exempelvis skolan, saknas särskilda registerförfattningar, och hanteringen av personuppgifter regleras av enbart personuppgiftslagen.

[61] Bilaga till protokoll nr III 5, vid regeringssammanträde den 29 oktober 2015, N2015/07455/EF.

De särskilda registerförfattningarna möjliggör oftast att personuppgifter hanteras på ett sätt som inte hade varit lagligen möjligt med stöd endast av personuppgiftslagen. Tanken med dessa regler är att möjliggöra sådan hantering av personuppgifter som myndigheterna behöver för att kunna utföra sina arbetsuppgifter, samtidigt som regelverket ska beakta de enskildas behov av skydd för sin personliga integritet.

Även offentlighets- och sekretesslagen (2009:400) och 2 kap. 6 § regeringsformen är av stor betydelse för att skydda den enskildes personliga integritet i samband med e-förvaltning.

På området finns även regler som inte har som syfte att skydda den enskildes personliga integritet, utan som i stället ska skapa insyn och transparens i förvaltningen. Hit hör förstås bestämmelserna om handlingsoffentlighet i tryckfrihetsförordningen, men också den s.k. PSI-lagen, dvs. lagen om vidareutnyttjande av handlingar från den offentliga förvaltningen. Arkivlagen (1990:782) med anslutande författningar har bevarande som huvudregel, men innehåller också bestämmelser om gallring, exempelvis föreskrivs i 7 kap. 1 § Riksarkivets föreskrifter och allmänna råd om arkiv hos statliga myndigheter (RA-FS 1991:1) att myndigheten fortlöpande ska pröva förutsättningarna för gallring. Bestämmelser om gallring i en registerförfattning har företräde framför arkivregelverket.

Betänkandet *Myndighetsdatalag*[62] innehåller en översiktlig kartläggning och kategorisering av de olika registerförfattningarna. Betänkandet visar på att registerförfattningar kan se ut på många olika sätt, både till innehåll och till uppbyggnad. I betänkandet föreslås att registerförfattningarna på sikt ska ersättas av en enda myndighetsdatalag.

11.3 Kommitténs samlade bedömning av området

Digitaliseringen i den offentliga förvaltningen har redan skapat betydande värden i form av bättre service till medborgarna och en effektivare förvaltning. Nyttoeffekten av de olika företeelserna i e-förvaltningen varierar emellertid till art och omfång. Det finns även stora variationer i riskerna för den personliga integriteten som företeelserna innebär.

[62] Informationshanteringsutredningens betänkande *Myndighetsdatalag*, SOU 2015:39.

Inom såväl statlig som kommunal förvaltning hanterar myndigheterna ett stort antal uppgifter om enskilda. Många gånger rör det sig om uppgifter som är känsliga i personuppgiftslagens mening, t.ex. om hälsa, eller som på annat sätt är närgångna och därmed integritetskänsliga, t.ex. uppgifter om enskildas inkomster, sociala problem, skuldsättningar och familjeförhållanden.

Oftast har de enskilda inget inflytande över myndigheternas hantering – den görs i regel utan deras samtycke. Det innebär att det vilar ett särskilt ansvar på det allmänna att se till att uppgifter bara hanteras när det verkligen är nödvändigt för att förvaltningen ska kunna utföra sitt uppdrag, och att se till att hanteringen är så säker som möjligt.

Teknikutvecklingen gör det möjligt för den offentliga förvaltningen att utveckla och effektivisera sin hantering av personuppgifter. Det innebär för det första en möjlighet att öka spridningen och vidareanvändningen av uppgifter, dvs. att öka hanteringen rent generellt. Men för det andra innebär utvecklingen också en möjlighet att skydda uppgifterna på ett bättre sätt genom att använda tekniker som stärker den personliga integriteten, t.ex. anonymisering.[63] Dessa två möjligheter går i praktiken ofta att förverkliga samtidigt.

En generell iakttagelse som kommittén gör är dock att myndigheter och regeringen fokuserar sitt utvecklings- och författningsarbete på den första möjligheten, medan man arbetar betydligt mindre på den andra. Det innebär att offentlig sektor riskerar att bygga in egenskaper i system, arbetsformer och i författningar, som kan bli mycket svåra och dyra att ändra på, om följderna för den personliga integriteten visar sig bli allvarliga.

Informationshantering inom och mellan olika myndigheter

Myndigheterna hanterar i dag fler uppgifter om enskilda än någonsin tidigare. Det finns i dag teknik som gör det enkelt att sprida, vidareanvända och sambearbeta uppgifter, såväl inom en myndighet som myndigheter emellan, eller mellan myndighet och enskilda.

Redan komplexiteten och de tekniska utmaningarna i några av de system som byggts upp för att dela information, kan innebära att utvecklingsresurserna används enbart åt funktionalitet och inte till

[63] Se vidare i bilaga 4 om integritetsskyddande teknik.

att analysera frågor som är av betydelse för integritetsskyddet. Det förekommer att frågor om t.ex. personuppgiftsansvar, behörighetstilldelning och förenlighet med registerförfattningar behandlas långt senare i utvecklingsprocessen – först när systemet tagits i skarp drift eller inte alls. Anmärkningsvärt är också att det i dessa sammanhang kan finnas brister i viljan hos myndigheter att ta ansvar för både hanteringen av och säkerheten för uppgifter om enskilda personer.

Faktorer som i detta sammanhang är av betydelse för risken för den personliga integriteten, är att det hos vissa myndigheter finns databaser som omfattar hela eller en stor del av befolkningen med uppgifter som kan vara mycket integritetskänsliga. Uppgifter kan spridas till handläggare, inom den egna myndigheten eller på en annan myndighet, som egentligen inte behöver kunna ta del av uppgifterna för att utföra sitt arbete. Enskilda kan i regel inte motsätta sig att deras uppgifter hanteras av myndigheterna. Vi anser därför att den ökade informationsdelningen inom och mellan myndigheter innebär en påtaglig risk för den personliga integriteten.

Samtidigt måste också beaktas att det finns en stor potential för att dessa företeelser både kan användas för att ge bättre service till allmänheten och för att effektivisera förvaltningen.

Informationsutbyte med enskilda

När det gäller e-tjänster som direkt vänder sig till enskilda, exempelvis s.k. egna utrymmen hos myndigheterna, anser kommittén att det finns en viss risk för den personliga integriteten. Faktorer som här är av betydelse för risken för den personliga integriteten, består främst i oklarheter kring personuppgiftsansvaret och i att e-tjänsterna kan ges en teknisk utformning som inte ger ett tillräckligt gott skydd för uppgifterna. Uppgifter kan spridas av misstag eller efter ett antagonistiskt angrepp (hacker-attack) riktat mot myndigheten.

Samtidigt måste också beaktas att det finns en tydlig potential för att sådana tjänster kan vara till stor och direkt nytta för enskilda personer.

Emellertid har vi noterat att myndigheter när det gäller vissa företeelser har en benägenhet att lägga över personuppgiftsansvaret på den enskilde. Det gäller till exempel möjligheten att använda smstjänster eller e-post i kontakten med en myndighet. Det innebär att

myndigheten inte fullt ut tar ansvar för att uppgifterna hanteras bara för de avsedda ändamålen och på ett tillräckligt säkert sätt. Den enskilde förväntas ta ansvar för en hantering som de flesta inte förmår överblicka i sin helhet. När sådana försök till förskjutning av ansvaret förekommer, kan det enligt kommitténs mening medföra att risken potentiellt ökar för den personliga integriteten.

Myndigheter med uppgifter i molnet och bristen på beställarkompetens

Vi har i avsnitt 21.1 om molntjänster gått igenom både risker och fördelar med användningen av molntjänster generellt. Dessa gäller i högsta grad även för myndigheter. Faktorer som för myndigheter är av särskild betydelse för risken för den personliga integriteten, är att myndigheterna kan hantera ett stort antal personuppgifter som kan vara mycket integritetskänsliga, ingå i allmänna handlingar och även omfattas av sekretess. Vidare måste myndigheter veta hur relevanta register- och arkivförfattningar ska tillämpas. Även andra integritetsskyddande regler kan vara av betydelse för myndigheterna, som exempelvis säkerhetsskyddslagen och Myndighetens för samhällsskydd och beredskap föreskrifter om informationssäkerhet hos statliga myndigheter. Många små myndigheter saknar kompetens att välja rätt slags molntjänst som fungerar juridiskt och säkerhetsmässigt för just den aktuella verksamheten. Vi anser att dessa faktorer sammantagna medför att det för myndigheter finns allvarliga risker med molntjänster, i synnerhet i s.k. publika moln (uttrycket förklaras närmare i avsnitt 21.1 om molntjänster).

Samtidigt måste också beaktas att det finns en stor potential för att effektivisera förvaltningen med hjälp av molntjänster, dvs. genom att låta företag lagra och hantera myndigheters data.[64]

Rent generellt för alla slags tjänster inom e-förvaltningen anser vi att det innebär en påtaglig risk för den personliga integriteten, att det alltjämt konstateras stora bister i myndigheters kompetens avseende

[64] Pensionsmyndigheten utvecklar i en nyligen utgiven rapport de potentiella fördelarna för statliga myndigheter med molntjänster, se *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015.

juridik, informationssäkerhet och kravställning, samtidigt som myndigheterna förväntas börja använda och utveckla nya system och tjänster.

Myndigheter i sociala medier och med gilla-knappar på webben

Faktorer som i detta sammanhang är av betydelse för risken för den personliga integriteten, är att det finns myndigheter som i förhållande till sociala medier präglas av ett visst mått av naivitet. Myndigheter inser inte alltid att de i onödan kan hjälpa sociala medier, deras samarbetsparter eller företagen bakom sökmotorerna, att kartlägga vad allmänheten gör på nätet. När myndighetens kunskap om detta är begränsad, får besökarna på webbplatsen naturligtvis inte heller tillräckligt med information om att uppgifter om deras aktiviteter på nätet kommer att lämnas ut till företag i tredje land för andra ändamål än att möjliggöra deras besök på myndighetens webbplats. Myndigheternas användning av tjänster från sociala medier och sökmotorföretagen (t.ex. att ha myndighetskonton eller gilla-knappar på den egna webbplatsen), kan innebära att integritetskänsliga personuppgifter lämnas ut till företag i tredje land, även om detta troligen bara görs undantagsvis. Sammanfattningsvis anser vi att myndigheternas användning av tjänster från sociala medier och sökmotorföretagen innebär en viss risk för den personliga integriteten.

Samtidigt är det viktigt att myndigheter kan använda sig av olika media och metoder för att informera brett och effektivt om sina verksamheter, i synnerhet som verksamheterna kan medföra både rättigheter och skyldigheter för den enskilde.

PSI-lagstiftningen

I likhet med PSI-utredningen anser vi att insatserna för att öka spridningen av information från myndigheter till resten av samhället, i kombination med en svårtillämpad och delvis oklar lagstiftning (i första hand PSI-lagstiftningen) innebär en påtaglig risk för den personliga integriteten.

Medborgarprofilering och kontroller på nätet

Av stort intresse för integritetsskyddet är sådan kontrollverksamhet hos myndigheter, som syftar till att i förväg bedöma vilken sannolikhet det finns för att en viss individ ska begå någon form av felaktighet. Av betydelse för risken för den personliga integriteten är att denna kontrollverksamhet präglas av frånvaro av transparens i förhållande till allmänheten. Detsamma gäller för myndigheters efterforskande verksamhet på öppna eller slutna delar av nätet. Här finns också en rad juridiska, bl.a. grundlagsrelaterade, frågetecken, både avseende de interna kontrollerna och kontrollerna på nätet. Vi anser därför att dessa kontrollverksamheter innebär allvarliga risker för den personliga integritetet.

Samtidigt måste också beaktas att det är synnerligen angeläget, både ur det allmännas och ur medborgarnas perspektiv, att myndigheterna på ett effektivt sätt kan använda sig av egna data och av nätet för att förebygga misstag och oegentligheter.

Informationssäkerhet

De brister i myndigheters informationssäkerhet som vid upprepade tillfällen har konstaterats av flera olika kontrollinstanser, måste sägas medföra en allvarlig risk för den personliga integriteten. Av betydelse i sammanhanget är förstås att myndigheterna hanterar en stor mängd uppgifter som kan vara både känsliga och närgångna och därmed synnerligen skyddsvärda. Brister i informationssäkerheten kan också rent generellt försämra allmänhetens tillit till den offentliga förvaltningen.

Kapitel 22, Informationssäkerhet och integritet, innehåller en redogörelse för informationssäkerhetens betydelse för skyddet av den personliga integriteten.

Brister i regelverket

Brister i regelverket för hantering av personuppgifter inom e-förvaltningen uppmärksammades redan år 2007 av Integritetsskyddskommittén. Kommittén pekade på att det var en genomgående brist att konsekvenserna för den enskildes integritetsskydd inte

hade analyserats och beaktats tillräckligt i arbetet, som under senare år har bedrivits för att underlätta myndigheters möjligheter att använda ny teknik och för att främja ett ökat informationsutbyte mellan myndigheter. I den mån överväganden av detta slag förekommit, menade kommittén att de inte dokumenterats tillräckligt i förarbetena till lagstiftningen.[65]

Även E-delegationen har i sitt slutbetänkande uppmärksammat att det finns brister i regleringen av förutsättningarna för en effektiv e-förvaltning och ett välavvägt integritetsskydd. E-delegationen bedömer att detta även påverkar enskildas tilltro till myndigheterna, vilket innebär att det är angeläget att regeringen har ett helhetsperspektiv när resultaten av tillsatta utredningar bereds.[66] Även Datainspektionen pekar i sina remissvar regelbundet på brister i nya författningsförslag när det gäller integritetsskyddet.[67]

Vår analys av e-förvaltningen utgår i detta delbetänkande från företeelser som kan ha betydelse för den personliga integriteteten, snarare än från det rättsliga skyddet på området. Emellertid har, som framgår ovan, andra granskningar konstaterat systematiska brister i såväl det befintliga regelverket som i de förslag till nya författningar som framförs på området. Ett genomtänkt regelverk kan bidra till att skydda den personliga integriteten, genom att tydligt peka ut ramar för vad myndigheterna får och ska göra med uppgifterna. Ett sådant regelverk kan också bidra till att myndigheterna känner sig trygga att utveckla nya e-tjänster inom lagstiftningens ramar. Kommittén befarar emellertid att bristerna i regelverket för e-förvaltningen kan medföra försämringar i integritetsskyddet.

Datainspektionens roll

Under arbetets gång har flera myndigheter efterlyst tydligare och mer konkret vägledning från Datainspektionen i frågor som rör e-förvaltning och integritetsskydd. Vi avser att återkomma till Datainspektionens uppdrag i slutbetänkandet.

---

[65] Integritetsskyddskommitténs delbetänkande *Skyddet för den personliga integriteten – Kartläggning och analys*, SOU 2007:22.

[66] SOU 2015:66.

[67] Se t.ex. Datainspektionens remissvar den 4 maj 2015 avseende SOU 2015:5, En ny svensk tullagstiftning, myndighetens dnr 404-2015.

Sveriges världsledande roll

I regeringens digitala agenda och e-förvaltningsstrategi sägs att Sverige ska bli världsledande när det gäller digitalisering. Det finns dock inga uttalanden om att skyddet för den personliga integriteten också bör nå en liknande världsledande ställning. En sådan ambition för integritetsskyddet inom e-förvaltningen vore kanske inte orimlig, eftersom det inte alls behöver innebära ett onödigt försvårande av utveckling av nya tjänster som förbättrar servicen till de enskilda och effektiviserar förvaltningen.

Samordning och styrning av utvecklingen

Sammanfattningsvis kan sägas att alla initiativ inom e-förvaltningen – till nya arbetssätt, tillämpning av ny teknik eller ändringar i regelverket – präglas av regeringens höga ambitioner för att påskynda utvecklingen. Samtidigt visar redan kommitténs översiktliga granskning av integritetsrisker inom e-förvaltningen att det på flera punkter finns betydande brister när det gäller både integritetsskydd och informationssäkerhet. Det är också tydligt att det i dag inte finns någon aktör i offentlig sektor som både har övergripande kunskap om vad som händer inom området, och i realiteten utövar en övergripande styrning över e-förvaltningen. Som flera andra, exempelvis E-delegationen och Riksrevisionen, har påpekat, innebär avsaknaden av samordning och styrning en risk för att utvecklingen bromsas och inte uppnår de önskade service- och effektiviseringsnivåerna. Men det innebär också en allvarlig risk för att den personliga integriteten inte skyddas tillräckligt. Risken förstärks av att de satsningar regeringen nu gör för att förstärka samordning och styrning för att utveckla området, inte motsvaras av någon satsning för att förstärka integritetsskyddet inom e-förvaltningen, och inte heller innehåller några direktiv eller tankar kring hur både e-förvaltning och ett gott integritetsskydd ska utvecklas tillsammans i medborgarnas intresse.

12 Konsumentområdet

Kommitténs bedömning: Det finns allvarliga risker för konsumenters personliga integritet.

12.1 Inledning

12.1.1 Beskrivning av området

Det här kapitlet handlar om hur enskilda personer blir kartlagda när de i egenskap av konsumenter eller presumtiva konsumenter befinner sig på stan, i hemmet, på nätet eller i en fysisk butik.[1] Vidare berörs betaltransaktioner – vem som får veta vad konsumenten betalar för. I kapitlet berörs även vad produkterna eller tjänsterna efter köpet rapporterar in till tillverkare och andra intressenter, samt om nya organisationsformer och affärsmodeller som innebär nya utmaningar för integritetsskyddet.

Många olika aktörer är av skilda anledningar intresserade av de elektroniska spår som konsumenter ger upphov till, gärna redan innan de enskilda själva vet om att de kommer bli konsumenter. Det finns självklart ett stort intresse för våra elektroniska spår hos de företag som vill sälja sina produkter eller tjänster, men även sökmotorer, webbplatser, reklamföretag, sociala medier, datamäklare och ibland även myndigheter, vill av olika skäl veta mer om hur vi beter oss när vi handlar eller lockas att handla.

[1] Det är i viss mån en förenkling att tala om konsumenter, eftersom en konsument i dag inte sällan samtidigt även är producent, genom att ändra en produkt eller tjänst eller använda en tjänst för att producera något. På nätet yttrar sig detta t.ex. genom att enskilda skapar och delar innehåll i form av text, film och bilder. Den dubbla rollen betecknas ibland som ”prosument”. Medieutredningen använder beteckningen ”medieborgare”, se avsnitt 12.6 i detta kapitel.

12.1.2 Internetekonomin

Personuppgifternas stora kommersiella värde har resulterat i ett utvecklat och intrikat system av olika datakällor, aktörer, flöden och affärsmodeller, vilka sammantagna ibland kallas för internetekonomin eller övervakningsekonomin (eng. *surveillance economy*).[2] Vid surfande på webben, användning av mobila enheter (t.ex. telefoner och surfplattor), appar och kroppsnära teknologi, genereras, lagras och sprids personuppgifter som är av stort intresse för bl.a. marknadsföring och utveckling av nya tjänster.

Tidigare delades konsumenter in i relativt grova målgrupper till vilka marknadsföring kunde riktas. I dag säljs och köps i stället enskilda konsumenters uppgifter på individnivå på den globala annonsmarknaden. Ju mer detaljerade uppgifterna är om den enskildes vanor, intressen, kontaktnät och aktuella livssituation, desto bättre för näringsidkaren.[3] Uppgifterna prissätts också på individnivå. Det finns exempelvis beräkningar som visar att genomsnittspriset för basuppgifter om en konsument (ålder, kön och plats) uppgår till cirka 0,0005 USD. Om den enskilde befinner sig i vissa betydelsefulla skeden i livet, blir uppgifterna dyrare. Graviditet, bilköp eller skilsmässa ökar exempelvis marknadsvärdet avsevärt. Särskilt eftertraktade och dyra är uppgifter om enskildas hälsoproblem och läkemedelsintag, då priset uppskattats till 0,26 USD per person.[4]

Redan något så vardagligt som att läsa tidningen på nätet innebär att ett mycket stort antal aktörer får ta del av uppgifter om läsaren. När en läsare går in på en tidnings webbplats, kontaktas automatiskt en annonsserver som uppmanar tidningens webbplats att fylla sina annonsytor med reklam. Tidningen skickar då en förfrågan till en s.k. annonsbörs. Förfrågan innehåller vissa upplysningar om läsaren, baserade bl.a. på vilka artiklar han eller hon visat intresse för eller på uppgifter som följt med vid inloggning på tidningens hemsida. Det kan t.ex. röra sig om den enskildes IP-adress, geografiska placering,

[2] Uttrycket övervakningsekonomi används exempelvis i norska Teknologirådets och Datatilsynets gemensamma rapport *Personvern 2016 – tilstand og trender*, publicerad i januari 2016.

[3] Norska Datatilsynets rapport *Personopplysninger og det digitale annonsemarkedet*, publicerad den 3 november 2015.

[4] Emily Steel, Callum Locke, Emily Cadman och Ben Freese, *How much is your personal data worth?*, publicerad den 12 juni 2013 på www.ft.com.

inkomst, kön och förmodade eller visade intressen. På annonsbörsen får sedan olika annonsörer bjuda på reklamplats riktad till den enskilde läsaren. Den som lägger det högsta budet vinner och får placera sina annonser på tidningens hemsida när den laddas ner av läsaren. Allt detta görs helt automatiskt och inom loppet av en bråkdels sekund.

De inblandade aktörerna är många. Ett besök på en webbsida kan i praktiken innebära att personuppgifter hanteras av uppemot ett hundratal olika aktörer. I första ledet finns leverantörer av innehållstjänster (tidningar, nyhetsportaler, sociala medier, sökmotorer och en mångfald av appar) som finansierar sina tjänster genom att sälja annonsplatser. I andra änden återfinns de som köper annonsplatserna. Däremellan finns annonsbörser och datamäklare. Datamäklare (eng. *data brokers*) är företag som har som affärsidé att samla in personuppgifter och sälja dem vidare, exempelvis paketerade som konsumentprofiler. En konsumentprofil kan innehålla uppgifter om t.ex. den enskildes livsstil och intressen. Uppgifterna kan komma från vitt skilda källor: sociala medier, offentliga register eller andra företags kundregister.

De största datamäklarna är från USA, bl.a. Acxiom, Experian och Datalogix. Dessa företag samlar inte bara in uppgifter om personer i USA. Exempelvis Axciom uppges ha uppgifter om 700 miljoner personer från olika delar av världen, med i genomsnitt 3 000 uppgifter om varje enskild person i databasen.[5] Bisnode och Experian är exempel på datamäklare som finns i Sverige.

12.1.3 Regelverk och tillsyn

Hantering av personuppgifter avseende handel och marknadsföring regleras av olika författningar, i huvudsak i enlighet med följande:

- personuppgiftslagen (1998:204),
- lagen (2003:389)om elektronisk kommunikation,
- lagen (1994:1512)om avtalsvillkor i konsumentförhållanden, och
- produktansvarslagen (1992:18).

[5] Norska Teknologirådets och Datatilsynets gemensamma rapport *Personvern 2016 – tilstand og trender*, januari 2016.

I första hand följande tillsynsmyndigheter kontrollerar hanteringen av personuppgifter i konsumentsammanhang:

– Datainspektionen (utövar tillsyn enligt personuppgiftslagen),
– Post- och telestyrelsen (utövar tillsyn över integritetsskyddet vid användning av elektroniska kommunikationstjänster, dvs. tillämpningen av 6 kap. lagen om elektronisk kommunikation),
– Konsumentverket (utövar tillsyn enligt lagen om avtalsvillkor i konsumentförhållanden) och
– Konsumentombudsmannen (kan utfärda förelägganden och inleda rättsprocesser mot företag som bryter mot lagen om avtalsvillkor i konsumentförhållanden).

Därtill utövar Justitieombudsmannen och i viss mån Justitiekanslern tillsyn över det allmännas verksamhet, och polis och åklagare utreder misstänkta brott.

Den enskilde som anser att hennes eller hans uppgifter hanterats på ett felaktigt sätt, kan således vända sig till olika tillsynsmyndigheter med ett klagomål. Beroende på vad klagomålet rör, är det olika myndigheter som ansvarar för tillsynen. Exempelvis ansvarar Datainspektionen för frågor som handlar om vilka uppgifter om kunderna som får hanteras och hur länge de får sparas. Post- och telestyrelsen ansvarar för frågor om hur samtycke inhämtas avseende placering av kakor på kundernas utrustning. Konsumentverket och Konsumentombudsmannen ansvarar för frågor om oskäliga avtalsvillkor. Även intressenter som exempelvis konsumentorganisationer kan anmäla brott och brister i t.ex. avtalsvillkor till myndigheter.

Vidare finns det en möjlighet för den enskilde kunden att begära skadestånd för den skada som hon eller han anser sig ha lidit på grund av integritetsintrång, och att då väcka talan vid allmän domstol.

12.2 Kartläggning på nätet – IP-adresser, kakor och digitala fingeravtryck

12.2.1 Företeelserna

Surfande på nätet genererar olika slags spår från den enskilde användaren (webbplatsbesökaren), även om besökaren inte genomför något köp eller fyller i något formulär.

Det finns en rad olika sätt att kartlägga vilka sajter en användare besöker och därmed vad han eller hon intresserar sig för.

12.2.2 Sökmotorer

Alla sökmotorer, som exempelvis Google, Bing, Duckduckgo, Yahoo och Baidu, fungerar i princip på samma sätt: En sökrobot (dvs. en slags programvara) besöker webbplatser automatiskt och samlar in all den information som hittas där, i form av text, dokument, bilder, ljud, filmer och även uppgifter om på vilken server webbplatsen finns och annan metadata. I nästa steg analyseras och lagras den information som hittats för att slutligen kunna fungera som sökresultat när någon gör en sökning. Tillsammans kallas detta för att sökmotorn indexerar webben.

Hur indexeringen utförs är en viktig del i hur bra en sökmotor upplevs fungera. Ju större index, dvs. större innehåll, desto större är chansen att det någon letar efter med sökmotorn kommer upp bland sökresultaten. Även algoritmerna i sökmotorn, som avgör hur de hittade webbsidorna ska rangordnas för användaren, är av stor betydelse.

När en sökning genomförs är givetvis de söktermer som användaren anger i sökrutan viktiga. Men även andra faktorer vägs in. Den IP-adress som användarens dator eller mobila enhet har, ger en ungefärlig uppskattning av var i världen personen i fråga befinner sig, och kan även kopplas till tidigare sökhistorik. Andra data som också kan utnyttjas för att avgöra vilka sökträffar som ska visas för just den aktuella användaren, är till exempel vilken webbläsare och vilket operativsystem användaren har.

Sökmotorerna kan också visa sökresultat från källor som användarna inte förväntar sig ska vara indexerade. Hit kan sociala medier höra, där företagen bakom tjänsterna ibland gör innehåll tillgängligt för sökmotorer. Vidare kan metadata göra information på webben

sökbar på sätt som inte är uppenbara. Hit hör exempelvis GPS-taggning av bilder eller inlägg i sociala medier. Om sådana uppgifter finns tillgängliga, blir det inte bara möjligt att söka efter innehållet i en statusuppdatering, utan också att leta efter bilder, statusuppdateringar eller annat som gjorts från en specifik plats.

De flesta sökmotorer som indexerar den öppna delen av webben är gratis att använda, i likhet med många andra tjänster på nätet. Intäkterna kommer i stället ofta från annonsörer. Ju mer kunskap om användarna en tjänsteleverantör har, desto större möjligheter finns att sälja annonsplatser. Med ökad kunskap kommer möjligheten att ge annonsörerna bättre kontroll över vem som får se deras annonser.

Filterbubblan

Sedan år 2011 har begreppet *filterbubbla* diskuterats. Begreppet myntades av författaren och debattören Eli Pariser som argumenterar för att algoritmer som syftar till att personanpassa tjänster på nätet, kan åstadkomma stor skada. Algoritmerna säkerställer att användarna bara får se mer av det man redan är intresserad av, eller som ständigt bekräftar den uppfattning av världen som man redan har intagit.

Filterbubblan är en följd av den ökande individanpassningen av tjänster på nätet och kan i sin tur medföra isolerande och på sikt diskriminerande effekter för konsumenter. Ibland talar man i stället för filterbubblor om ”ekokammare”.[6] Som exempel på företeelsen kan nämnas att resultaten av en Googlesökning visas först sedan Google ”tvättat” resultatet och då vägt in många olika faktorer om användaren rörande exempelvis användarens webbläsare, användarens sökhistorik, geografiska position och så vidare. Det innebär att en användare inte kan hitta (och därmed i praktiken utesluts från) sådana produkter, tjänster och erbjudanden som enligt sökmotorn inte skulle passa för användaren i fråga. Företeelsen är också av betydelse när det gäller mediekonsumtion. Exempelvis påverkas Facebookanvändares mediekonsumtion både av deras sociala nätverk och av hur Facebook väljer att prioritera olika nyheter. Tendensen att bara ta del av nyheter som ens gelikar intresserar sig för, förstärks av

[6] Sam Sundberg, *Filterbubblan sluter sig allt tätare om oss*, publicerad i SvD den 10 mars 2015.

Facebooks inverkan på mediaflödet och innebär att användaren kan komma att missa mycket annat. Möjligheten att upptäcka något nytt kan i vissa fall, paradoxalt nog, begränsas genom användningen av sociala medier.[7]

12.2.3 IP-adresser

En IP-adress är ”den tekniska adress som datorer (och enheter som skrivare, routrar, etc.) använder för att kommunicera via nätverk”.[8] Förkortningen IP står för *Internet Protocol.* En IP-adress består av siffror och är på teknisk väg kopplad till ett mer hanterligt domännamn genom adresseringssystemet Domain Name System (DNS). DNS gör det möjligt för en användare att knappa in bokstäver som adress till en webbplats. Exempelvis är IIS (Stiftelsen för internetinfrastrukturs) domännamn *.iis* kopplat till en IP-adress som skrivs ut som 212.247.7.229.

IP-adressen till en privat användares dator är ofta dynamisk, vilket betyder att datorn kan få en ny IP-adress varje gång användaren kopplar upp sig på nätet. En IP-adress talar dock alltid om vilken internetleverantör som datorn använder, varifrån den kopplat upp sig och en del annan teknisk information. Det finns en uppsjö med webbtjänster som tillhandahåller möjligheten att översätta ett domännamn till en IP-adress, eller tvärtom, och som även talar om vilken som är användarens IP-adress.[9]

Webbsurfande kräver i allmänhet att båda parter (besökaren och webbplatsen) känner till varandras IP-adresser. Undantaget är om användaren använder sig av någon anonymiseringstjänst som exempelvis TOR-nätverket.[10]

---

[7] Företeelsen undersöks exempelvis i Eytan Bakshy, Solomon Messing och Lada Adamic, *Exposure to ideologically diverse news and opinion on Facebook*, Science, 7 maj 2015.

[8] Internetstiftelsens i Sverige internetguide nr 25, *Källkritik på Internet*, av Kristina Alexanderson (publicerad 2012). Förkortningen IP står för engelskans Internet Protocol.

[9] Internetstiftelsens i Sverige internetguide nr 25, *Källkritik på Internet*, av Kristina Alexanderson (publicerad 2012).

[10] Tor-nätverket är en grupp av servrar som driftas av frivilliga och som används för att kommunicera via virtuella tunnlar, för att på så vis låta användarna vara anonyma på nätet, se https://www.torproject.org/

12.2.4 Kakor

En kaka (cookie) är en liten textfil som den besökta webbplatsen sparar på besökarens dator (med eller utan föregående information och samtycke). Kakan kan sedan förse webbplatsen med information om besökaren. Varje kaka innehåller bl.a. en egen identitetsbeteckning och används för att webbplatsen ska kunna veta vad den enskilde besökaren gör eller tidigare har gjort på webbplatsen. Exempelvis används kakor på webbplatser som säljer varor för att göra det smidigt att handla. Med hjälp av kakor kan webbplatsen hålla reda på vilka varor besökaren har lagt i sin elektroniska varukorg.

Post- och telestyrelsen har en webbtjänst som ger en ungefärlig uppfattning om hur många och vilka slags kakor som placeras på besökarens dator vid besök på en viss webbplats.[11] Även den ideella föreningen dataskydd.net har en liknande webbtjänst, som förutom att analysera kakor även undersöker om en webbplats använder sig av dataskyddande funktioner som exempelvis kryptering vid kommunikation med besökarens webbläsare.[12]

Vissa kakor, s.k. tredjepartskakor, placeras vid besök på en webbplats, men härrör från någon annan än den som ansvarar för webbplatsen. Exempelvis kan företag som har köpt annonsplats på webbplatsen placera tredjepartskakor på besökarnas datorer, utan att besökaren behöver klicka på annonsen. Det annonserande företaget får då veta varje gång besökaren kommer in på en webbplats som har annonser från företaget. Vidare kan den som ansvarar för webbplatsen anlita en extern statistiktjänst för att ta fram fakta om besökarna. Statistikföretaget kan då få information om alla besökare på webbplatser som använder sig av företagets statistiktjänst. Ett exempel på en mycket vanlig statistiktjänst är Google Analytics.

De flesta webbplatser sätter ett antal kakor i besökarens dator. Exempelvis kunde i mars 2015 konstateras att Aftonbladet satte 35 kakor från 9 olika domäner på sin startsida, Expressen satte 63 kakor från 19 domäner på sin och Nyheter24 satte 151 kakor från 55 domäner.

[11] http://e-tjanster.pts.se/internet/kakor/
[12] https://webbkoll.dataskydd.net/sv/

Genom samarbete mellan olika annonsföretag går det att skapa en god, sammantagen bild av den enskilde besökarens surfvanor som kan sägas avslöja besökarens intressen på nätet. Med hjälp av den informationen kan ett annonsföretag välja vilken produkt eller tjänst som den ska visa för besökaren i fråga i sina annonser. Detta kallas ibland för beteendestyrd annonsering.[13]

Emellertid är webbläsarna i dag ofta förinställda på att inte acceptera tredjepartskakor. Det leder till att det blir allt färre enskilda besökare som kan kartläggas med hjälp av tredjepartskakor.

En undersökning av hur kakor placeras genomfördes under år 2014 av Artikel 29-gruppen i samarbete med åtta nationella myndigheter med ansvar för e-komfrågor.[14] Sammanlagt undersöktes 478 webbplatser inom områdena e-handel, media och offentlig sektor. De 478 undersökta webbplatserna placerade tillsammans ut 16 555 kakor dvs. i genomsnitt 34,6 kakor per webbplats. Cirka 70 procent av alla kakor var tredjepartskakor. Några kakor hade en giltighet på 8 000 år, men det vanligaste var en giltighetstid på mellan 1 och 2 år. En relativt liten grupp om 25 olika domäner stod för hälften av alla tredjepartskakor. Undersökningen visade också att det inte var ovanligt att webbplatser varken informerar besökarna om kakorna eller inhämtar samtycke till att placera kakor, trots de legala kraven som finns på detta.

12.2.5 Digitala fingeravtryck

Även om användningen av kakor har stängts av i webbläsaren, lämnar webbläsarna s.k. ”digitala fingeravtryck” vid surfning (på engelska används uttrycken *device fingerprint, machine fingerprint eller browser fingerprint*). Även vid anonym surfning lämnar webbläsare ifrån sig uppgifter till de sajter som besöks. Bland annat talar webbläsaren om att den är Internet Explorer eller Firefox eller Safari eller någon annan läsare. Den talar dessutom om vilken version de är, vilket operativsystem som finns på besökarens dator, om några insticks-

[13] Artikel 29-gruppens yttrande 2/2010 *om beteendebaserad reklam på Internet.*
[14] Artikel 29-gruppens WP 229, *Cookie Sweep Combined Analysis – Report*, den 3 februari 2015.

program har installerats i webbläsaren, om besökaren använder några speciella typsnitt och annat. Sammantaget gör dessa uppgifter att besökarens dator blir mer eller mindre unik.[15]

Webben (World Wide Web) är uppbyggd på ett sätt som innebär att webbplatser hämtar sitt innehåll inte bara från den som ansvarar för platsen, utan även från många andra parter. Det innebär att även dessa tredje parter har möjlighet att ta del av besökarnas digitala fingeravtryck.[16]

12.2.6 Det skyddande regelverket

Enligt lagen om elektronisk kommunikation ska alla som besöker en webbplats med kakor som huvudregel få tillgång till information om att webbplatsen innehåller kakor och ändamålet med användningen av kakor. Besökaren ska också ge sitt samtycke till att kakor används på detta sätt.

Dessa bestämmelser i lagen om elektronisk kommunikation grundar sig på artikel 5.3 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.[17]

Direktivets bestämmelser om information och samtycke ska enligt Artikel 29-gruppen även tillämpas på digitala fingeravtryck.[18] En sådan tolkning av direktivet bör medföra att bestämmelserna i lagen om elektronisk kommunikation om information och samtycke (6 kap. 18 §) även ska tillämpas på digitala fingeravtryck.

Den fortsatta hanteringen av informationen i kakan eller det digitala fingeravtrycket, hos den som ansvarar för webbplatsen, hos annonsören eller den som på annat sätt blir ansvarig för hanteringen, omfattas av bestämmelserna i personuppgiftslagen. Det framgår av 6 kap. 2 § lagen om elektronisk kommunikation. I Artikel 29-gruppens vägledning för tillämpningen tydliggörs förhållandet mellan de bägge bakomliggande direktiven.[19]

---

[15] Datainspektionens tidskrift Magazin direkt, nr 1, 2010.

[16] Artikel 29-gruppens yttrande 9/2014 *on the application of Directive 2002/58/EC to device fingerprinting*.

[17] Det s.k. e-Privacy-direktivet, som ändrats genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009.

[18] Artikel 29-gruppens yttrande 9/2014 *on the application of Directive 2002/58/EC to device fingerprinting*.

[19] Artikel 29-gruppens yttrande 2/2010 *om beteendebaserad reklam på Internet.*

Enligt den praxis som vuxit fram vid tillämpningen av personuppgiftslagen, ska IP-adresser behandlas som personuppgifter i lagens mening.

12.2.7 Risker för den personliga integriteten

För e-handelsföretag blir det allt viktigare att göra sina webbplatser individanpassade och bekväma för besökaren. Det är svårt att behålla kunder på nätet, vilket stärker behovet av att veta mer om de besökare som en gång har hittat till webbplatsen.

Det finns därmed ett starkt, kommersiellt intresse hos många webbplatser att få veta så mycket som möjligt om sina besökare med hjälp av olika tekniker. Det finns dock inte ett lika starkt intresse för att göra besökarna medvetna om den kartläggning som faktiskt görs.

Det räcker med en timmes surfande på olika webbplatser för att upptäcka att många webbplatser inte lämnar information eller inhämtar ett godtagbart samtycke innan kakor placeras på besökarens dator.

Ännu mer sällan ges besökaren någon information om hur andra uppgifter såsom IP-adresser eller digitala fingeravtryck används av webbplatsen.

Det finns alltså klara brister i vad den enskilde får veta om hanteringen och i dennes möjlighet att påverka, trots att det finns ett relativt tydligt regelverk att förhålla sig till.

Hantering av uppgifter hos en enstaka webbplats är i de flesta fall endast till fördel för besökaren och helt harmlös. Men när sammanställningar görs av hela annonsnätverk om en enskild besökares surfvanor, innebär det en kartläggning av den enskilde som kan uppfattas som närgången, särskilt som besöken även kan avslöja känsliga uppgifter om besökaren, såsom politisk övertygelse eller sexuella preferenser. I ett känt exempel lyckades forskare identifiera enskilda personer med utgångspunkt i drygt 100 miljoner avidentifierade filmbedömningar. Återidentifieringen kunde göras med hjälp av källor på nätet. Förutom återidentifieringen menade forskarna att de för vissa av personerna kunde dra slutsatser om deras privata och integritetskänsliga intressen.[20]

[20] Arvind Narayanan och Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, Proceedings of the 2008 IEEE Symposium on Security and Privacy.

Uppgifter om surfvanor kan också i allt större utsträckning identifieras och sambearbetas med andra datasamlingar. Även teleoperatörer hanterar stora mängder kunduppgifter, och det finns röster i branschen som efterlyser lättnader i regelverken för att möjliggöra att dessa uppgifter används för nya ändamål.[21]

Kartläggning på nätet har ur ett integritetsskyddsperspektiv beskrivits av Artikel 29-gruppen på följande sätt:

> Annonsnätverk tar fram prediktiva profiler genom att använda en kombination av spårningsteknik, cookiebaserad teknik och programvara för informationsutvinning. Det går att dra slutsatser om kön och åldersgrupp genom att analysera vilka webbsidor den registrerade besöker och vilka annonser han eller hon intresserar sig för. Profilen som baseras på analys av de cookies som lagras på den registrerades terminalutrustning kan kompletteras med samlade data från surfvanorna hos registrerade användare som visar ett liknande beteendemönster i andra sammanhang. Reklamsystem på internet klassificerar ofta de registrerade i segment, antingen utifrån intresseområden eller utifrån marknadsföringskategorier (exempelvis ”trädgård”, ”kroppsvård”, ”elektronik” osv.). Var den registrerade befinner sig är också en viktig faktor för målgruppsprofileringen. Det går att dra slutsatser om var användaren befinner sig exempelvis från datorns IP-adress och WiFi-anslutningspunkter. Ytterligare information om platsen kan samlas in från andra källor och användas för profileringen.[22]

Post- och telestyrelsen inledde i februari 2014 en granskning av hur reglerna om kakor i lagen om elektronisk kommunikation följs. Syftet med granskningen är att få fram praxis och vägledning om t.ex. vilken information som ska lämnas till besökare och hur besökarnas samtycke ska inhämtas. Resultatet av granskningen förväntas under år 2016 och kan bli av stor betydelse för både existerande affärsmodeller och för hur webbplatser fungerar och är uppbyggda.

[21] Katelyn Lunders och Magnus Franklin, *Mobile operators seek Big Data prize in slimmed-down e-Privacy law*, publicerad den 12 april 2016 i M-Lex.

[22] Artikel 29-gruppens yttrande 2/2010 *om beteendebaserad reklam på Internet.*

12.3 Positionering

12.3.1 Företeelsen

När enskilda personer rör sig i den fysiska världen lämnar de allt fler digitala spår efter sig. Spåren lämnas genom teknik som många bär med sig, som t.ex. mobiltelefoner eller smarta kort till lokaltrafiken. Spåren lämnas också genom teknik som finns utplacerad i stadsmiljön, som t.ex. övervakningskameror, i bland kombinerade med program för bildanalys. Om utrustningen är placerad tillräckligt tätt, skapas ett finmaskigt nät som gör det möjligt att följa enskilda individers rörelser över större områden. Precisionen i kartläggningen av enskildas rörelser varierar beroende på syfte. System för automatiska vägtullar läser av registreringsskyltar på de fordon som passerar tullstationerna och samlar på så vis in information om rörelserna i en stad på makronivå. En butiksägare som vill veta hur kunderna rör sig bland hyllorna kan montera små Bluetooth-sändare som kommunicerar med kundernas mobiltelefoner, och på så sätt få rörelsemönster på mikronivå.

12.3.2 Wifi-tracking[23]

Smarta telefoner vars wifi-sändare inte har stängts av, söker hela tiden efter trådlösa nätverk genom att sända ut uppgifter med bl.a. telefonens unika MAC-adress. Uppgifterna kan tas emot av anslutningspunkter i exempelvis publika trådlösa nätverk eller av anslutningspunkter som upprättas bara i syfte att ta emot signalerna. Genom att känna till var anslutningspunkterna är placerade, blir det möjligt att lokalisera telefonen som sände ut uppgifterna, samt att följa hur telefonen rör sig mellan olika anslutningspunkter i nätverket. Sådan lokalisering går ibland under benämningen *wifi-tracking*.

Tekniken möjliggör en så detaljerad kartläggning att den används av butiker som vill veta hur kunderna rör sig inne i butiken, framför vilka hyllor de stannar, om det är en återkommande kund, hur länge

[23] Wifi används numera oftast som beteckning på trådlösa, lokala nätverk för signalöverföring (s.k. WLAN).

kunden tillbringar inne i butiken osv. Enligt uppgifter i media använder sig vissa butiker i Sverige av wifi-tracking för att få veta hur kunder rör sig i butikerna.[24]

Tekniken används också i kommuner, eller närmare bestämt av samverkansorganisationer (s.k. citysamverkan) där handlare och fastighetsägare ingår och kommunerna finns med som samarbetspartners. I ett tiotal svenska kommuner planerade man under år 2014 att börja använda tekniken för att få veta mer om hur besökare rör sig genom städerna.[25]

Datainspektionen granskade därför under år 2014 användningen av wifi-tracking i Västerås (genom Västerås Citysamverkan).[26] Granskningen visade att de så kallade MAC-adresser, som samlades in, är personuppgifter och att Västerås Citysamverkan därför måste följa reglerna i personuppgiftslagen. Datainspektionen kom bl.a. fram till att behandlingen av personuppgifterna innebar en sådan kartläggning av enskilda, att dessas intresse av skydd mot kränkningar av den personliga integriteten vägde tyngre än Västerås Citysamverkans intresse av att behandla personuppgifterna. De enskilda måste också få information om vem som samlade in deras uppgifter och varför.

I stort sett alla smarta telefoner i dag är försedda med wifi-teknik, och många användare har ständigt wifi-funktionen aktiverad på sina telefoner. Det innebär att wifi-tracking möjliggör positionering och kartläggning av en relativt stor del av befolkningen.

Både wifi- och Bluetooth-teknikanvändning innebär således en risk för omfattande kartläggning av innehavarnas rörelsemönster, utan att de berörda enskilda har en aning om det och därmed inte heller kan vidta åtgärder för att skydda sig. Det finns också en risk för att användaren varken får veta vilka som hanterar uppgifter om honom eller henne eller vilka uppgifter som hanteras.

[24] *Köpvanor kartläggs med hjälp av wifi*, publicerad den 31 juli 2914 på www.dn.se

[25] Sofia Nordén och Mikael Grill Pettersson, *Städer vill kartlägga dig genom din mobil*, publicerad den 29 september 2014 på www.svt.se.

[26] Datainspektionens beslut den 22 juni 2015 i dnr 2729-2014. Västerås Citysamverkan vidtog efter beslutet åtgärder som innebar att det inte längre gick att följa hur enskilda personer rör sig i Västerås stadskärna.

12.3.3 Bluetooth low energy

En relativt ny teknisk lösning är små Bluetooth-sändare som har utvecklats för att finnas i t.ex. offentliga miljöer och där kommunicera med mobiltelefoner som kommer inom räckhåll. Tanken är bland annat att använda tekniken för att skicka reklamerbjudanden, men också att registrera hur besökare eller kunder rör sig i exempelvis ett köpcenter. Sändarna gör det möjligt att skapa en motsvarighet till webbens cookies i den fysiska världen, och kan skicka erbjudanden till återkommande besökare.

Bluetooth är en standard för trådlös kommunikation för överföring av data över korta avstånd. Tekniken finns i smarta telefoner och har blivit mycket vanlig för att koppla ihop telefonerna med olika andra enheter, som exempelvis hörsnäckor och persondatorer. Alla enheter med Bluetoothfunktionerna (eller wifi-funktionerna) aktiverade kan spåras när de sänder ut uppgifter om enheten.

Version 4 av Bluetooth-standarden innehåller en särskild funktion för lågenergienheter, kallad för *Bluetooth low energy* (BLE). BLE möjliggör för enheter att kommunicera med varandra med en energiåtgång som bara är en bråkdel av vad som krävs för vanlig Bluetooth-kommunikation. Det antas att BLE-enheter kan vara i drift i upp till ett år med ström bara från knappcellsbatterier. BLE tillåter emellertid inte överföring av exempelvis ljud, utan möjliggör endast överföring av små datapaket.

Tidiga med att utnyttja BLE var Apple som år 2013 tog fram sin s.k. *iBeacon.* I Apples tillämpning skickar små sändare (*beacons*, dvs. fyrar) ut datapaket av liten storlek som mobiltelefonen kan känna igen. Telefonen svarar sedan sändaren med motsvarande små datapaket. Apples fyrar kan fungera både med iPhones och vissa Androidtelefoner. *iBeacon*-tekniken har en rad olika användningar. Exempelvis kan fyrarna positionera mobilerna, sända individanpassade reklamerbjudanden till mobilen, och möjliggör även trådlösa betalningar som exempelvis PayPals betaltjänst *PayPal Beacon.* Den är tänkt som ett smidigare och energisnålare alternativ till betalkortterminaler och NFC-baserade betalsystem (*Near field communica-*

tion, se nedan delavsnitt 12.4 om elektroniska betalningar).[27] *iBeacon*-tekniken har en räckvidd på cirka 50 meter vilket vida överstiger NFC-baserade tekniker.

BLE-enheter är billiga både att tillverka och att ha i drift. Det gör BLE till en attraktiv kommunikationsteknik.

Det finns redan i dag en stor mängd apparater på marknaden med BLE-teknik inbyggd. Troligen kommer BLE-funktionalitet inom kort vara mycket vanlig i mobiltelefoner, smarta TV-apparater, wearables och även i bilar.

BLE-enheter är små och mycket energisnåla och kan därför enkelt byggas in i produkter och kommunicera med mobiltelefoner utan att produktens innehavare ser eller på annat sätt blir medveten om det. Det finns också en risk för s.k. *Bluejacking* som innebär att en sändare skickar oönskade meddelanden med skadlig kod till en enhet med aktiverad Bluetooth-funktion.

I ett samarbete med hjälp av Bluetooth mellan en dagstidning och en matvaruproducent användes begreppet ”fysisk retargeting” för att beskriva reklamkampanjen.[28] Retargeting är ett begrepp hämtat från webben, och används för att beskriva det som alla nätanvändare har varit med om: Efter att ha tittat på varor i en nätbutik dyker det direkt upp annonser för samma produkter på exempelvis Facebook. Detta är möjligt eftersom cookies utnyttjas för att annonssystemen ska veta vilka varor en användare tidigare har visat intresse för. Det som dagstidningen och matvaruproducenten gjorde, var att utnyttja Bluetooth-sändare på ett liknande sätt. Matvaruproducenten ställde upp en foodtruck, där förbipasserande bjöds på gratis varuprover. Men i bilen fanns också Bluetooth-sändare som letade efter dagstidningens app i gratisätarnas telefoner, utan att någon information om detta gavs. Senare skickades ett meddelande till gratisätarnas telefoner, där mottagarna erbjöds att hämta ytterligare ett varuprov i en butik.

[27] Leena Rao, *PayPal Debuts Its Newest Hardware, Beacon, A Bluetooth LE Enabled Device For Hands-Free Check Ins And Payments*, publicerad den 9 september 2013 på www.techcrunch.com.

[28] Erik Wisterberg, *Aftonbladet: ”Vi är först i Sverige med fysisk retargeting*”, publicerad den 22 januari 2015 på www.dagensmedia.se

12.3.4 RFID

RFID är en förkortning för *Radio-frequency Identification*. Som framgår av namnet är det en radiobaserad teknik för att identifiera och positionera det föremål som RFID-taggen är fäst vid och för att lagra viss annan information om förmålet i fråga.

En RFID-tagg består av ett minne som innehåller informationen och en antenn som kan användas för att skicka informationen till en s.k. läsare (ett slags aktiv mottagare).

Det finns passiva taggar som saknar eget batteri och drivs av en radiosignal från läsaren, dvs. att de behöver väckas till liv av mottagaren. Passiva taggar kan väckas till liv många år efter att de placerades på ett föremål men har relativt kort räckvidd (upp till några meter). Passiva RFID-taggar kan göras mycket små och kapslas in i material som passar för användningsområdet, exempelvis kan de finnas i självhäftande plast- eller pappersetiketter. Det är även vanligt att kapsla in RFID-taggar i ett sterilt glashölje, som är så litet att det ryms inuti en injektionsnål, för märkning av boskap, hästar och sällskapsdjur.[29]

Aktiva RFID-taggar har eget batteri och därmed längre räckvidd (upp till flera hundra meter) och är större än passiva taggar. De behöver inte vänta på att väckas till liv av en läsare, utan kan själva påbörja informationsöverföringen.

Det finns ett stort antal olika RFID-kretsar på marknaden. De enklaste lagrar endast ett unikt serienummer, ofta 64 bitar långt, som bränns in vid tillverkningen och därefter endast kan läsas. Mer avancerade kretsar kan ersätta inte bara magnetkort och streckkoder, utan även smarta kort och erbjuder dubbelriktad kommunikation med kryptering och ett skrivbart minne.[30]

RFID-tekniken ansluts ofta till större system och till internet via någon form av terminalserver.

RFID-taggar används numera i många olika sammanhang, och är vanliga när det gäller att följa varor som är under förflyttning hos handlare eller hos transportföretag. Men RFID-teknik används även

[29] Internetstiftelsens i Sverige internetguide, nr 19 (version 1.0 2009) *Uppkopplade prylar – En rapport om Internets framtid och hur apparaterna går online*, av David Boda, Linus Brohult, Erik Mörner, Tomas Nilsson och Roman Pixell.

[30] Internetstiftelsens i Sverige internetguide, nr 19 (version 1.0 2009) *Uppkopplade prylar – En rapport om Internets framtid och hur apparaterna går online*, av David Boda, Linus Brohult, Erik Mörner, Tomas Nilsson och Roman Pixell.

för märkning av kläder i butik, i elektroniska biljetter i kollektivtrafiken, i elektroniska nycklar, för märkning av både bagage och boardingkort på flygplatser, i pass, i biblioteksböcker och så vidare.

Således kommer RFID-taggar till användning på en rad olika områden, och de uppfattas som en billig och praktisk teknik.

Även RFID-teknik möjliggör kartläggning av enskilda personer – både genom positionering och genom att RFID-taggen kan lagra och avslöja mer detaljerad information om en person eller ett föremål i personens närhet. Det finns en risk för att de enskilda inte har en aning om och hur de kan kartläggas med hjälp av RFID-taggar.

Kartläggningen kan göras både avsiktligen och oavsiktligen. Ett exempel på det förra är att RFID-taggar på boardingkort kan avslöja hur passagerare rör sig på en flygplats och därmed vilka andra resenärer de möter och umgås med. Ett exempel på det senare är om RFID-taggar inte avlägsnas från en produkt när den säljs till enskilda konsumenter. En klädaffär skulle då kunna läsa av de gamla taggarna i en besökares kläder och på så sätt fastställa vilken prisgrupp kläderna tillhör för att därmed göra antaganden om vilken slags konsument besökaren är.

RFID-taggar som lagrar känslig information om enskilda kan läcka informationen om den inte är skyddad på ett tillräckligt sätt. Detta skulle kunna inträffa om RFID-taggar används inom hälso- och sjukvården för att lagra hälsorelaterad information om sina bärare.

RFID-teknik är användbar och relativt billig och kan därför i framtiden antas öka i användning på många olika områden.

Artikel 29-gruppen har uppmärksammat RFID-teknikens risker för den personliga integriteten.[31]

[31] WP 105, *Working document on data protection issues related to RFID technology,* den 19 januari 2005.

12.3.5 GPS[32]

Vid sidan av den positionering av en mobiltelefon som görs i mobilnäten har telefonerna själva också teknik som gör det möjligt att avgöra var i världen de befinner sig. Alla moderna telefoner i dag har en inbyggd GPS, förutom att också wifi-funktionen kan användas för positionering. Det finns appar att installera som loggar eller i realtid rapporterar var telefonen befinner sig. I somliga av apparna går det att ställa in så kallade geo-fence, vilket är virtuella staket där ett larm ska skickas om telefonen passerar gränsen.

Vidare har både iPhone och de telefoner som använder operativsystemet Android, funktioner som automatiskt registrerar var de befinner sig. Detta används bland annat i reklamsyfte, för att användaren ska få annonser baserade på sin fysiska position. Det används också för att ta fram sökresultat så att användaren ska få förslag baserade på sin fysiska position, och för att användaren ska kunna hitta sin telefon om den har tappats bort. Men det innebär också att en person som får tillgång till telefonen (eller till uppgifter från telefonen som lagras i en molntjänst) kan se var den egentlige användaren brukar befinna sig eller till och med kan spåra användarens rörelser bakåt i tiden och se var han eller hon befunnit sig timme för timme.

Till detta kommer möjligheten att förse andra föremål eller personer med en GPS-sändare. Det finns exempelvis batteridrivna GPS-sändare att placera i ett barns ryggsäck, eller GPS-sändare att sätta i en bil för att automatiskt skapa färdloggar och därmed spåra hur bilen rör sig.

12.3.6 Mobilnät

I en uppmärksammad artikel i slutet av sommaren 2015 kunde Dagens Nyheter i detalj visa hur mycket information mobiloperatörerna har om hur deras kunder rör sig. Reportern hade begärt ut den information som hans operatör hade lagrat under det senaste halvåret. Det är så länge informationen, enligt datalagringsdirektivet, ska

[32] Förkortningen GPS står för engelskans *Global Positioning System*, och är enligt Nationalencyklopedins beskrivning ett satellitnavigationssystem för bestämning av positioner med mycket stor noggrannhet hos exempelvis båtar, flygplan, landfordon eller till och med personer.

få finnas kvar innan den får raderas. Informationen får bara begäras ut av brottsbekämpande myndigheter, något som enligt DN:s granskning gjordes för 2 022 brottsmisstänkta personer under 2014.[33]

Över 10 000 datapunkter om var DN-reporterns telefon hade befunnit sig fanns lagrade hos operatören, i snitt en var 25:e minut dygnet runt. Uppgifterna innehåller koordinater för de basstationer som mobiltelefonen vid varje tillfälle är uppkopplad till. Eftersom basstationerna i stadsmiljö sitter väldigt tätt innebär det att uppgifterna är mycket detaljerade. I en granskning som gjordes någon månad tidigare hade Dagens Nyheter avslöjat ett fall hos en teleoperatör, där en anställd förföljde en kund via dennes mobiltelefon.

12.3.7 Det skyddande regelverket

Enligt huvudregeln i 6 kap. 18 § lagen om elektronisk kommunikation ska alla som besöker en webbplats med kakor få tillgång till information om att webbplatsen innehåller kakor och ändamålet med användningen av kakor. Besökaren ska också ge sitt samtycke till att kakor används på detta sätt.

Bestämmelsen ska dock enligt Datainspektionen inte tillämpas på överföringen av datapaket från och till mobiler vid wifi-tracking.[34]

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter i samband med positionering. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

12.3.8 Risker för den personliga integriteten

Den långtgående positionering som görs med hjälp av elektronisk utrustning som enskilda bär med sig eller som finns i omvärlden, innebär att det kan utföras en omfattande kartläggning av enskildas rörelsemönster. Kunskap om vilka platser den enskilde besöker, och när besöken görs, kan avslöja mycket om den enskildes intressen, vanor, sociala kontakter och en uppsjö av annan information om den enskilde.

[33] Kristoffer Örstadius och Linus Larsson, *Mobilen spårar dig – överallt*, publicerad den 31 augusti 2015 på www.dn.se.
[34] Datainspektionens beslut den 22 juni 2015 i dnr 2729-2014.

Den enskilde som inte är beredd att vidta radikala åtgärder – som att undvika platser som är övervakade, avstå från att använda modern utrustning eller att genomgående endast använda utrustning och tjänster som möjliggör anonymitet, kommer att få det allt svårare att värja sig mot vardagens alla positioneringstekniker.

12.4 Elektroniska betalningar

12.4.1 Företeelsen

Slaget om framtidens betalningslösningar blir allt mer intensivt. I flera år har det talats om alternativa betalningslösningar, med olika former av mobilbetalning som de främsta kandidaterna. Det är banker, kortföretag, it-företag och andra aktörer som tävlar om att bli den ledande och mest populära betalningslösningen. Samma utveckling kan ses både i Sverige och internationellt.[35]

Elektroniska betalningar kan göras i nätbutiker, fysiska butiker och mellan privatpersoner. Det finns en rad olika tekniska lösningar för digitala betalningar på marknaden.

De uppgifter som behöver utbytas för att genomföra betalningen, kan skickas över internet, i telenätet som sms eller direkt mellan enheterna genom NFC-teknik. Många lösningar involverar kundernas mobiltelefoner. Vanligen krävs då att kunden först laddar ner en app till telefonen.

NFC (Near field communication) är en överföringsmetod för kontaktlöst utbyte av data över korta sträckor, i allmänhet som mest 10 centimeter (det finns dock särskilda, mycket känsliga mottagare som kan avläsa signaler på ett avstånd av upp till en meter).

Både mobiltelefoner och betalkort kan ha en inbyggd NFC-krets och användas för elektroniska betalningar utan att det behövs en pinkod för att genomföra transaktionen.

Även i Sverige finns det företag som tillhandahåller tjänster för förmedling av elektroniska betalningar. I slutet av år 2013 granskade Datainspektionen fyra sådana företag. I avsnittet nedan om riskerna för den personliga integriteten, återkommer vi till resultatet av den granskningen.

[35] Martin Mederyd Hårdh, *Apple i ”betalningskrig” med Walmart*, publicerad den 28 oktober 2014 på www.svd.se och Pär Ivarsson, *Allt fler operatörer planerar mobilbetalning*, publicerad den 5 mars 2015 på www.sr.se.

I avsnitt 15.3 beskriver vi hanteringen av personuppgifter i samband med användningen av kreditkort och vid betaltransaktioner som görs över nätet.

12.4.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter i samband med digitala betalningar. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

12.4.3 Risker för den personliga integriteten

Överlag innebär elektroniska betalningar i jämförelse med kontantbetalningar helt nya möjligheter till kartläggning av kunder. Det är nu – i teorin och ofta även i praktiken – möjligt att koppla samman alla uppgifter om köparen, den köpta varan eller tjänsten, tidpunkten för köpet, platsen och i vilken butik som köpet genomfördes. Elektroniska betalningar mellan privatpersoner gör det också möjligt att kartlägga ekonomiska relationer och beroendeförhållanden av mer privat karaktär som inte involverar något köp. När det går att koppla samman uppgifter om riktad och individanpassad reklam på nätet, med uppgifter om faktiskt utförda köp, blir det också möjligt att på en mycket detaljerad nivå mäta effekten av marknadsföringsinsatser: köpte personen i fråga den marknadsförda produkten eller tjänsten?

I ett nyligen uppmärksammat forskningsprojekt kom en grupp forskare fram till att det med utgångspunkt i endast fyra ”anonyma” elektroniska betaltransaktioner är möjligt att identifiera en enskild köpare. I undersökningen analyserades kontokortstransaktioner från 1,1 miljoner personers köp i 10 000 affärer i ett och samma land under tre månaders tid. Underlaget innehöll varken namn, kreditkortsnummer, adresser eller exakta tider. Den enda information som forskarna hade att tillgå var köpets belopp, i vilken typ av affär köpet gjorts och en kod som representerade varje person. I nio av tio fall lyckades forskarna identifiera personen som gjort köpen. Identifieringen kunde göras med hjälp av bl.a. uppgifter om taxiresor

som läckt ut på nätet och andra uppgifter som de flesta personer genererar i dag, exempelvis från geolokaliserade tweets eller mobilappar som samlar in lokaliseringsdata.[36]

I ett berömt exempel från år 2012 visste matvarukedjan Target i USA att en av deras underåriga kunder var gravid, baserat på hennes köpbeteende, innan hennes familj ens hade fått veta det. Target hade räknat ut att gravida i en viss månad plötsligt ändrar sina köpvanor på några avgörande punkter. Exempelvis börjar många gravida köpa oparfymerade produkter och vissa koststillskott. Informationen om graviditeten var värdefull för Target, eftersom de då kunde ligga steget före alla andra som riktar marknadsföring till nyblivna föräldrar först när barnet är fött. I exemplet blev flickans föräldrar upprörda på Target eftersom de trodde att Target utan anledning skickat deras dotter babyrelaterad reklam. I sammanhanget förtjänar att uppmärksammas att Targets profilering inte gjordes med hjälp av amatörmässiga gissningar, utan baserades på ett omfattande och långvarigt arbete av statistiker och matematiker som haft stora databaser om kunderna att utgå från.[37] Target är inte unika med att göra så stora satsningar för att få mer kunskap om kunderna.

I förhållande till det skyddande regelverket, bör följande risker särskilt lyftas fram när det gäller elektroniska betalningar. Uppgifter om enskilda personer kan komma att hanteras för ändamål som de enskilda inte känner till eller har samtyckt till. Exempelvis kan företaget som förmedlar den elektroniska betalningen lämna ut uppgifter till tredje part utan att ge tillräcklig information till de enskilda och utan att inhämta ett verkligt samtycke eller ge okända tredjepartsapplikationer åtkomst till uppgifter.

Vidare finns det en risk för att de enskilda inte kan få information om vem som faktiskt hanterar deras uppgifter och vilka uppgifter dessa okända personuppgiftsansvariga får åtkomst till. Det kan också förekomma att uppgifter om enskilda användare sprids till underleverantörer utanför EES i länder med en dataskyddsreglering som inte når upp till en tillfredsställande skyddsnivå.

[36] Sophia Nilsson, *Forskarlarm: Tre inköp avslöjar din identitet*, publicerad den 30 januari 2015 på www.idg.se, samt John Bohannon, *Credit card study blows holes in anonymity*, Science, 30 januari 2015, vol. 347, nr 6221, s. 468.

[37] Charles Duhigg, *How Companies Learn Your Secrets*, publicerad den 16 februari 2012 på www.nytimes.com.

Dessa risker konstaterades också reellt föreligga vid Datainspektionens ovan nämnda granskning av fyra företag som tillhandahåller tjänster för förmedling av elektroniska betalningar.[38]

I granskningen riktade Datainspektionen kritik mot att kunduppgifter från ett företag lämnades ut till ett annat företag utanför EES (som antogs vara personuppgiftsbiträde, fastän avtal om detta saknades) utan att det fanns tillräckliga begränsningar i avtalet med detta andra företag om vad kunduppgifterna fick användas till. Vidare skulle tvister med det andra företaget lösas med tillämpning av den federala och delstatliga lagstiftning som gäller i Kalifornien. Det personuppgiftsansvariga företaget fick heller inte veta i vad mån kunduppgifterna skulle lämnas vidare från det andra företaget till dess underleverantörer. Det sagda innebar förstås att de enskilda kunderna i Sverige, vars uppgifter det var frågan om, fick veta ännu mindre och hade ännu mindre kontroll över hanteringen än det svenska företaget.

Betallösningar som använder sig av NFC-teknik innebär vissa särskilda risker. Enheter som har NFC-funktionen aktiverad kommunicerar med varandra utan andra begränsningar än sådana som är inbyggda i programvaran som finns installerad på enheten. Det innebär en risk för att enheten, utan innehavarens samtycke eller vetskap, via NFC instrueras att lämna exempelvis ut de kontaktlistor som finns lagrade på telefonen.

Eftersom en enhet med NFC-funktionen aktiverad sänder ut radiosignaler hela tiden, finns det också en risk för ständig och detaljerad positionering av enhetens innehavare, även när inga köp genomförs.

12.5 Sakernas internet (Internet of Things)

12.5.1 Företeelsen

En kort men i detta sammanhang tillräcklig definition av sakernas internet (på engelska *internet of things*, förkortat IoT) skulle kunna vara ”saker” och vardagsföremål såsom apparater eller sensorer (med undantag för datorer, smarta telefoner och surfplattor) som över

[38] Datainspektionens beslut den 9 juni 2014 i dnr 1822-2013, 1823-2013, 1826-2013 och 1838-2013. De ovan nämnda bristerna förelåg i en molntjänst för e-post som ett av de granskade företagen använde i sin kundtjänst.

internet kopplar ihop sig med varandra, kommunicerar med varandra eller överför information mellan varandra – utan mänsklig inblandning (eller med mänsklig inblandning bara i enstaka led).[39]

I stort sett alla föremål kan göras smarta och därmed ingå i sakernas internet. Det som behövs är att föremålet förses med sensorer (som kan mäta olika saker som temperatur eller rörelse osv.), processorer (som kan räkna det uppmätta eller göra nödvändiga beräkningar med värdena), lagringsenheter (som kan spara mätvärden och beräkningar för senare användning), nätuppkoppling (som gör det möjligt att överföra data och instruktioner) och batterier (som gör att det smarta förmålet faktiskt fungerar).[40]

Exempel på uppkopplade saker i dag är s.k. kroppsnära teknologi (eng. *wearables*), bestående av sensorer som är inbyggda i föremål som är lätta att bära med sig, som armband, eller i vardagsföremål som alla redan är vana att alltid bära med sig, som klockor och glasögon.

Andra exempel är personvågar, kylskåp, dörrlås, lampor. Det kan också handla om sensorer som mäter rörelser, luftfuktighet, temperatur. Det handlar också om uppkopplade bilar, klockor, aktivitetsarmband, kameror och många, många andra saker. Via nätverk, oftast internet, kommunicerar sakerna med andra saker, men också med människor.

Bland icke-bärbara saker kan nämnas olika uppkopplade enheter i hemmet. Det finns exempelvis företag som tagit fram sensorer för ytterdörren som automatiskt aktiverar termostaten i hemmet, så att värmen dras ned när det inte är någon i huset. Andra exempel är smart belysning som kan stängas av och sättas på via en app i mobiltelefonen och kaffemaskiner som också kan aktiveras via en app. Det finns även sensorer som med hjälp av rörvibrationer och tryckförändringar ska kunna mäta vattenförbrukningen i hemmet för att visa hur mycket vatten som går åt till toalettbesök, till duschning, till vattning i trädgården och så vidare.

Ett annat viktigt område för sakernas internet är olika slags medicintekniska produkter, alltifrån konsumentens egen blodtrycksmätare som via mobilen och en app lagrar uppgifter i molnet, till avancerad och dyrbar, utrustning på sjukhus, som t.ex. magnetkameror och

[39] Rapporten *Internet of Things – Privacy & Security in a Connected World*, FTC Staff- Report, januari 2015.

[40] Norska Teknologirådets och Datatilsynets gemensamma rapport *Personvern 2015 – tillstand og trender*, januari 2015.

kirurgiska robotar, som kan skicka uppgifter över nätet om utrustningens prestanda till sin tillverkare och ta emot uppdateringar av programvaran.

Sakernas internet har i dagsläget slagit igenom på bred front inom vissa delar av industrin, men har ännu inte nått samma spridning bland produkter i konsumentledet. Emellertid finns det anledning att anta att det uppkopplade hemmet kommer att bli allt vanligare i och med att konsumentelektronik i allt större utsträckning får möjlighet att koppla upp sig mot nätet.

De siffror som brukar nämnas när framtiden för sakernas internet kommer på tal är förstås relativt osäkra. Somliga menar exempelvis att det år 2020 kommer finnas 50 miljarder saker som är uppkopplade i världen.[41]

12.5.2 Uppkopplade fordon

Ett område av sakernas internet som kan sägas leda utvecklingen, är uppkopplade bilar och lastbilar. Moderna fordon är försedda med ett antal mätare och datorer som uppkopplade mot nätet rapporterar in data om fordonets framförande och tillstånd.

Här finns det åtskilliga frågor om datahanteringen som ännu är oklara för både konsumenterna och branschen. Det handlar om alltifrån vem som har rätt att använda uppgifterna (som är en värdefull tillgång för att kunna utveckla och kontrollera fordonen och även för att kunna utföra rätt sorts underhåll), till frågor om information till de enskilda, samtycke, vidareanvändning och skydd av uppgifterna.

Särskilt dataintensiv är den pågående utvecklingen av självkörande bilar och lastbilar. För att kunna konstruera de lösningar som låter en dator i stället för en mänsklig förare fatta beslut om hur fordonet ska framföras, krävs stora mängder ny teknik. Fordonen utrustas med ett ännu större antal sensorer än vanliga fordon, bland annat i form av kameror och radarutrustning som tillsammans ger en bild av vad som händer i omgivningen. Radiokommunikation, både med bilar i omedelbara närheten och med andra fordon via tjänster på nätet är också en viktig del. Utvecklingen kommer att ske stegvis och redan

[41] *Nationell agenda internet of things – Summering av projektet IoT Sverige*, Kungl. Ingenjörsvetenskapsakademien (IVA), 2013.

finns en del sådan teknik i fordon som rullar på vägarna i dag. Hit hör bland annat adaptiva farthållare som anpassar sig till framförvarande bil och utrustning som ser till att bilen inte lämnar sitt körfält.

Företag i Sverige anses ligga långt framme i utvecklingen av självkörande fordon. T.ex. finns *Drive Me* som är ett storskaligt försök för självkörande personbilar. Planen är att 100 sådana Volvo-bilar ska rulla på större vägar runt Göteborg år 2017.

När varje fordon som rullar på vägarna blir en rörlig sensorplattform innebär det inte bara att den kan köra själv utan också att detaljerad data om väderförhållanden och trafiksituation kan samlas in och användas som underlag i de beslut som datorn fattar om rutt eller hastighet. Den information som samlas in kommer inte bara att användas för framförandet av det aktuella fordonet, informationen kommer också att få andra tillämpningsområden.

För närvarande analyseras frågan om självkörande bilar och lastbilar i Utredningen om självkörande fordon på väg.[42] Utredaren ska analysera vilka regelförändringar som behövs för en introduktion av förarstödjande teknik och för helt eller delvis självkörande fordon på väg. I uppdraget ingår att analysera problem och möjligheter vad avser frågor om integritet och datasäkerhet vid lagring och användning av information från självkörande fordon. I mars 2016 presenterade utredningen ett delbetänkande.[43]

12.5.3 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för den hantering av personuppgifter som förekommer i och mellan uppkopplade saker. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

Även produktansvarslagen skulle kunna bli tillämplig eftersom den ger en möjlighet till skadestånd för person- eller sakskada som en produkt har orsakat på grund av en säkerhetsbrist.

[42] N 2015:07.

[43] Utredningens om självkörande bilar på väg delbetänkande *Vägen till självkörande fordon – försöksverksamhet*, SOU 2016:28.

12.5.4 Risker för den personliga integriteten

Den samlade mängden av uppgifter från alla uppkopplade saker möjliggör en detaljerad kartläggning av användarna som omfattar en stor del av deras privata vanor. Sensorer kan samla in uppgifter som var för sig inte är känsliga, men som tillsammans med data från andra källor kan ge information om personers hälsa, ekonomi och mycket privata vanor. Ett exempel som ibland nämns är att uppgifter om puls och andning tillsammans gör det möjligt att dra slutsatser om alkohol- eller koffeinintag, eller om personen i fråga tagit heroin eller kokain.[44]

Mängden data som samlas in av uppkopplade saker kan bli väldigt omfattande. Det blir därmed svårt att på ett säkert sätt anonymisera informationen.

Sakernas internet kan ge upphov till oklarheter kring vem som faktiskt hanterar konsumenternas uppgifter, om det är tillverkarna (det kan vara flera inblandade i en och samma produkt), försäljaren eller någon underleverantör till tillverkaren eller försäljaren osv.

En stor poäng med sakernas internet är att de uppkopplade sakerna ska sköta sig själva, utan att dra uppmärksamhet till sig. Processerna ska underlätta användarnas vardag och ska inte ställa en massa krångliga frågor om användarvillkor eller haka upp sig genom att invänta samtycken. De uppkopplade sakerna saknar dessutom oftast skärmar eller liknande som skulle kunna användas för att visa användarvillkor eller för att låta saken fråga användaren vilken information som ska delas och därmed låta användaren göra informerade val. Allt detta försämrar förstås förutsättningarna när det gäller användarnas medvetenhet och vetskap om de dataflöden som sakernas internet involverar.

Det innebär i sin tur en risk för att uppgifter om enskilda konsumenter kan komma att hanteras för ändamål som konsumenterna inte har en aning om och inte har samtyckt till.

En bred spridning av sakernas internet innebär att konsumenterna kommer att behöva ta ställning till ett stort antal pågående personuppgiftsbehandlingar. Den situationen riskerar att snabbt bli oöver-

[44] Annamalai Natarajan m.fl. *Detecting Cocaine Use with Wearable Electrocardiogram Sensors Detecting Cocaine Use with Wearable Electrocardiogram Sensors*, UbiComp'13, September 8–12, 2013, Zurich, Switzerland.

skådlig för den enskilde konsumenten och kan resultera i att det blir ännu vanligare än i dag med ett slags lågkvalitativa samtycken som grundas på bristfällig information om den faktiska hanteringen.[45]

När det gäller användarvillkor är otydlighet ett problem som återkommer inom sakernas internet, precis som när det gäller många andra företeelser. Många gånger är det oklart vad tillverkaren samlar in och lagrar på egna servrar men också hur den informationen säljs vidare.[46]

När sakernas internet utvecklas och får fullt genomslag i konsumentledet, kan det bli närmast omöjligt att använda sig av nya produkter och tjänster utan att röja sin identitet och sina mycket privata vanor, vilket innebär att det blir mycket svårt att vara anonym. Det kan medföra särskilda problem för personer som lever med skyddade personuppgifter.

Det finns också risker som rör skyddet för personuppgifter som hanteras av uppkopplade saker. De flesta inbyggda sensorer i uppkopplade saker som finns på marknaden i dag, kan inte kryptera överföringen av uppgifter, eftersom sådan kryptering kräver mer ström än den som alstras i de batterier som driver sensorerna.[47]

Uppkopplade saker har ofta en begränsad livslängd. Det innebär ofta ett minskat incitament för tillverkaren att säkerhetsuppdatera produkterna, vilket kan leda till att enskilda använder produkter som är sårbara för hackerattacker. Den här sårbarheten öppnar exempelvis för s.k. *Drive-by scanning* som kan avslöja uppgifter om användarna för personer som förbereder brott eller för myndigheter som genomför olika sorts kontroller av hushållen.

I Sverige har Kungliga ingenjörsvetenskapsakademien med stöd av Vinnova (Verket för innovationssystem) tagit fram en agenda som beskriver en strategi och plan för hur Sverige ska bli en ledande nation inom ett antal branscher genom gemensam avancerad utveckling och användning av sakernas internet.[48]

Rapporten handlar om att påskynda utvecklingen av sakernas internet i Sverige. I rapporten sägs emellertid ytterst litet om vilken utveckling som är önskvärd när det gäller de enorma möjligheter till

[45] Artikel 29-gruppens yttrande 8/2014 *On the Recent Developments on the Internet of Things*.
[46] *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, av Scott R Peppet, i Texas Law Review Vol. 93:85.
[47] Artikel 29-gruppens yttrande 8/2014 *On the Recent Developments on the Internet of Things.*
[48] *Nationell agenda internet of things – Summering av projektet IoT Sverige*, Kungl. Ingenjörsvetenskapsakademien (IVA), 2013.

kartläggning av individer som sakernas internet rymmer, och hur man kan gå till väga för att försöka påverka utvecklingen i önskvärd riktning för att både möjliggöra sakernas internet och samtidigt så långt som möjligt undvika integritetsförluster. Frågan nämns kort på sidan åtta i rapporten:

> Ekosystemet kommer att utforma etiska regler som ska följas vid utveckling och drift av IoT-system. Bland annat kommer regler att sättas upp för när data ska raderas och endast metadata sparas. De säkerhetsteknologier som finns för att skydda information och ge tillgång till den som är behörig kommer att implementeras.

Vad som här ska förstås med ”ekosystem” förklaras inte närmare i rapporten utan endast med ett citat från Wikipedia.

Ur ett integritetsskyddsperspektiv finns det en fara med att, som föreslås i rapporten, satsa på utveckling och ökad användning av en teknik, och samtidigt utgå från att frågor om risker och regelverk som är förenade med tekniken kommer att lösa sig av sig själva.

Slutligen kan också noteras att sakernas internet som samlad företeelse inte har granskats ur ett integritetsskyddsperspektiv av någon tillsyns- eller expertmyndighet.

12.6 Mediekonsumtion

12.6.1 Företeelsen

Filmer, nyhetssändningar, tidningar, radio och böcker konsumeras alltmer sällan linjärt (dvs. inte när de sänds enligt de tider som anges i TV-tablån) eller på papper, utan på nätet när användaren själv väljer att ta del av materialet.

Enligt IIS:s (Internetstiftelsen i Sverige) internetsstatistik för år 2015 dominerar dock ännu traditionella medier som radio, TV och boken, över sina olika versioner på internet. Huvuddelen av lyssnar-, tittar- och lästiden ägnas åt medierna utanför nätet. Versionerna på internet utgör komplement till de traditionella formerna. Dagstidningar utgör emellertid ett undantag. Här har papperstidningens andel av den totala lästiden (papper plus internet) tydligt minskat. År 2013 stod papperstidningen för 76 procent av lästiden. År 2015 hade den tiden minskat till 60 procent.

Tecken på pågående förändringar av konsumtionsmönstren återfinns i olika undersökningar. När det gäller t.ex. strömmande tv-tjänster uppmättes under fjärde kvartalet 2015 den högsta siffran någonsin för sådana tjänster. Enligt mätningen tittade svenskarna under kvartalet i genomsnitt drygt 36 minuter per dag på online-TV.[49] Bakom ökningen låg i första hand amerikanska tjänster som Netflix och Youtube. Av undersökningen framgick att nästan 40 procent av svenskarna mellan 15 och 74 år tittade på online-tv en genomsnittlig dag under fjärde kvartalet 2015, vilket motsvarade nära 3 miljoner personer, och innebar en uppgång med 20 procent från år 2014.

Att konsumera media på nätet, dvs. att läsa, lyssna eller titta på nätet, innebär att användarens aktiviteter och val registreras, sparas och används för olika ändamål, exempelvis för att anpassa mediet till den individuelle användaren, både när det gäller vilket innehåll som presenteras och när det gäller att skräddarsy marknadsföring som ska kunna locka just den aktuella användaren. Det är också möjligt att följa upp den faktiska mediekonsumtionen på ett helt annat och mer tillförlitligt sätt än vad som är fallet med linjära medietjänster.

Nyhetskonsumtionen på nätet analyseras i Medieutredningens delbetänkande.[50] En del av den senare tidens skifte i konsumtionsmönster kan enligt Medieutredningen förklaras genom att nyheter allt mer läses eller ses i mobilen. En annan förändring är förskjutningen i var nyheter konsumeras, där det har skett en förflyttning till sociala medier.

Medieutredningen pekar på att förflyttningen till de sociala medierna innebär att det tillkommit nya arenor för det demokratiska samtalet, arenor som ägs av internationella, kommersiella storbolag:

> Dessa väljer, via hur de bygger sina algoritmer, vilket innehåll som synliggörs för olika individer. Enligt exempelvis Facebook sker det personaliserade urvalet av innehåll med utgångspunkt i användarnas beteendemönster.

En annan aspekt av förändringen som berörs av Medieutredningen, är att medielandskapet inte längre präglas av medier med informationsmonopol, som väljer ut vilka budskap som anses viktiga och presenterar innehållet för en väntande och förhållandevis passiv

[49] Uppgifterna kommer från en rapport från konsultbolaget Mediavision vilken återges i artikeln *Nya rekord för online-tv*, publicerad på di.se den 27 januari 2016.

[50] Medieutredningens delbetänkande *Medieborgarna & medierna, En digital värld av rättigheter, skyldigheter – möjligheter och ansvar*, SOU 2015:94.

publik. Medborgarna är i allt högre utsträckning också själva aktiva med att publicera och distribuera kvalitativt innehåll. De lämnar därmed den forna passiva rollen för att bli vad Medieutredningen valt att kalla ”medieborgare”.

Medieutredningen uppmärksammar att Google samlar in och analyserar data om flera miljarder individers beteenden för att kunna leverera ett individualiserat innehåll och individuella tjänster. Detsamma gäller för en ökande skara medieföretag. Användardata och individualisering har blivit essentiella komponenter för dagens – och framtidens – framgångsrika medieföretag.

Kombinationen av olika data om en användare, som geografisk position, vanor i form av exempelvis läshistorik, köpbeteende, och familjerelationer kan, kombinerat med automatiseringen av innehållsproduktionen, generera ett skräddarsytt innehåll i realtid.

Medieutredningen sammanfattar situationen när det gäller nyhetsmaterial med att konstatera att utvecklingen ”innebär en kraftig förskjutning av maktförhållanden: de digitala giganterna har tillskansat sig makt över yttrandefriheten”.

12.6.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter genom användning olika slags medier på nätet. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

En viktig begränsning i personuppgiftslagens tillämpning på detta område, är att lagen inte gäller vid kollision med bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Vidare behöver många av personuppgiftslagens bestämmelser inte tillämpas när det rör sig om en behandling av personuppgifter uteslutande för journalistiska ändamål.

12.6.3 Risker för den personliga integriteten

Den enskilde som förlägger sin mediekonsumtion till nätet, kartläggs beträffande sina intressen för nyheter, litteratur, film, politik och annat. Resultatet blir en kartläggning av mycket ingående natur som visar den enskildes högst privata intressen och preferenser.

Som framgår av avsnittet om internetekonomin ovan, är det många aktörer som hanterar uppgifter som den enskilde för olika ändamål. Ur den enskildes synvinkel framstår området som svåröverskådligt. Även i de fall när den enskilde faktiskt får information om hanteringen, är informationen ofta svår att tyda och kan innehålla vaga och vittomfattande formuleringar. Det är kort sagt mycket svårt för den enskilde att få heltäckande kunskap om hur uppgifterna hanteras. Den enskildes möjligheter att påverka minskar i motsvarande mån.

Även möjligheterna att avstå från digitala medier kommer i en snar framtid att minska, i takt med att medielandskapet ändras och att alltmer flyttas från den icke-digitala världen. Den som i framtiden vill konsumera medier, kommer i praktiken inte ha något annat val än att göra det på nätet och därmed ge ut sina uppgifter till mediaföretag, annonsörer, datamäklare och andra intressenter.

12.7 Smarta mätare

12.7.1 Företeelsen

Konsumtionen av el, vatten, gas eller värme mäts och debiteras oftast ner på hushållsnivå. Mer detaljerade mätning anses tillsammans med andra åtgärder kunna bidra bl.a. till minskad konsumtion.

Mätningarna görs allt oftare med mätare som är uppkopplade mot nätet och som kan mäta konsumtionen på en mycket detaljerad nivå och ange precis hur mycket som konsumeras och när konsumtionen äger rum. Mätarna kan även fjärravläsas och gör det möjligt att fjärravstänga tillförseln. De smarta mätarna gör det också möjligt att utveckla nya taxor och tjänster baserade på kundens konsumtionsprofil.

I Sverige har frågan om elmätare i s.k. smarta elnät varit föremål för särskilt intresse. Bland annat har regeringens tillsatt ett samordningsråd för smarta elnät, vilket efter sitt upphörande följts av ett

nationellt forum för smarta elnät. Samordningsrådet publicerade ett slutbetänkande, i vilket betydelsen av att skydda konsumenterans personliga integritet lyfts fram.[51]

Smarta elnät har definierats som ”elnät som kostnadseffektivt kan integrera beteenden och beslut hos alla användare som är anslutna till det – elproducenter, elkonsumenter och de som är både och – för att garantera ett hållbart kraftsystem med låga förluster och hög kvalitet, försörjningstrygghet och säkerhet”.[52]

På det tekniska planet är smarta elnät ett elnät som i ökad utsträckning utnyttjar it och kommunikationsteknik samt avancerad mätning, övervakning och styrning. Ett viktigt inslag är också insamling, bearbetning och analys av mycket stora datamängder genom avancerad beräkningsteknik och ny mjukvara.

Utvecklingen av smarta elnät innebär att mätdata och information kommer att samlas in med allt högre upplösning och med allt kortare tidsinternvall. När uppgifterna om enskildas elkonsumtion ökar, ökar också möjligheterna att kartlägga enskildas och företags förehavanden.

Att integritetsfrågan inte ska försummas har erfarenheter från Tyskland, Österrike och Nederländerna visat, där farhågor kring den personliga integriteten har försvårat uppbyggnaden av en infrastruktur för smart mätning. Opinionen har bl.a. medfört att det finns möjligheten att neka till installationen av smarta mätare för kunder, en s.k. ”opt-out” klausul.[53]

I Sverige pågår runt om i landet flera olika projekt med inriktning på smarta elnät. I betänkandet *Planera för effekt* nämns bl.a. Smart Grid Gotland, Norra Djurgårdsstaden i Stockholm, Stadsdelen Hyllie i Malmö, Kraftsamling smarta nät i Västra Götalandsregionen och GrowSmarter i Stockholm.[54]

Energimarknadsinspektionen har fått i uppdrag av regeringen att utreda och lämna förslag på en framtida modell för informationsutbyte på elmarknaden – om hur data ska kommuniceras mellan marknadsaktörer, var data ska lagras och hur data kan göras tillgängligt för olika aktörer. I detta syfte har myndigheten bl.a. tagit fram en rapport

[51] Samordningsrådets för smarta elnät slutbetänkande *Planera för effekt*, SOU 2014:84.

[52] Definition framtagen av samarbetsorganisationen för EU:s tillsynsmyndigheter för energimarknaderna, European Regulators Group for Electricity and Gas (ERGEG), återgiven i SOU 2014:84.

[53] SOU 2014:84.

[54] SOU 2014:84.

om en informationshanteringsmodell på den framtida svenska elmarknaden.[55] I rapporten föreslås en omfattande, central och obligatorisk hantering av uppgifter om samtliga elkunder i Sverige. Datainspektionen har i ett yttrande över rapporten pekat på flera frågetecken kring modellen. En centraliserad hantering av uppgifter om samtliga elkunder i Sverige kan enligt Datainspektionen få stora konsekvenser för den personliga integriteten. För att det överhuvudtaget ska gå att ta ställning till förslagen i rapporten är det enligt Datainspektionen nödvändigt att utförligt kartlägga och analysera vilka risker för den personliga integriteten som den föreslagna informationshanteringsmodellen kan medföra. För detta arbete kan det bl.a. vara nödvändigt att närmare definiera för vilka ändamål som personuppgifter kommer att behandlas, vilka personuppgifter som är relevanta och adekvata för dessa ändamål, hur länge uppgifterna behöver sparas för dessa ändamål, vilka som kommer att ha tillgång till de insamlade personuppgifterna och till vilka uppgifterna ska lämnas ut.[56]

I ett hem som är försett med en smart elmätare går det att ta reda på en hel del om vad som försiggår, t.ex. om hur dygnsrutinerna ser ut, när någon kommer hem och vad personen då gör, om den lagar mat eller tittar på TV. Vissa menar t.o.m. att det är möjligt att utifrån elkonsumtionen dra slutsatser om vad som visas på en TV-apparat.[57]

12.7.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter genom användning av smarta mätare. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

[55] Energimarknadsinspektionens rapport *Informationshanteringsmodell på den framtida svenska elmarknaden*, Ei R2014:16.

[56] Datainspektionen yttrande den 2 oktober 2014 i dnr 1773-2014.

[57] Miro Enev m.fl, *Televisions, video privacy and powerline electromagnetic interference*, CCS'11, October 17–21, 2011.

12.7.3 Risker för den personliga integriteten

Med hjälp av smarta mätare, kan det göras en mycket närgången kartläggning av vad som försiggår i hemmet, som för de flesta är den allra mest privata sfären. Det kan vara svårt för konsumenterna att föreställa sig hur mycket leverantörerna faktiskt kan lista ut om enskildas privata vanor utifrån bara konsumtionen av el, gas, vatten eller värme.

12.8 Appar[58]

12.8.1 Företeelsen

Appar är datorprogram som utvecklats för en specifik uppgift och som är inriktade på en särskild grupp av smarta enheter (som smarta telefoner, surfplattor och tv-apparater med internetanslutning).

Apparna organiserar informationen på ett sätt som är särskilt anpassat för enhetens specifika egenskaper. Apparna samverkar ofta nära med hårdvaran och det operativsystem som finns på enheterna.

Det finns hundratusentals olika appar att ladda ner från olika appbutiker för varje typ av smart enhet. Appar används till olika saker, som webbläsning, kommunikation (e-post, telefoni och meddelanden via internet), underhållning (spel, filmer/videoklipp, musik), socialt nätverkande, banktjänster och platsbaserade tjänster.

Enligt IIS internetstatistik för år 2015 har två av tre smartmobilanvändare (47 procent av befolkningen) börjat använda Mobilt BankID och nästan fyra av tio använder Swish. Fyra av tio (29 procent av befolkningen) publicerar åtminstone ibland var de är via mobilen och drygt var tredje (27 procent av befolkningen) har någon form av sensorförsedd utrustning som via en app registrerar hur de tränar.

Enligt IIS internetstatistik för år 2014 hör just hälso- och träningsappar till populära nyheter som presenterats under de senaste åren. Det är unga kvinnor som är flitigast att använda hälso- och träningsappar, långt mer än unga män. Hälften av de unga kvinnorna i åldern 16–35 år har en sådan app.

[58] Detta delavsnitt bygger i huvudsak på Artikel 29-gruppens yttrande 2/2013 *om appar på smarta enheter*.

Mest använd enligt IIS statistik för år 2014 är Facebook-appen som används av 43 procent av alla personer som någon gång laddar ner appar. Sedan kommer bankappar (27 procent), tidningsappar (23 procent) väderappar (21 procent), spelappar (23 procent), Instagramappen (18 procent), Spotifyappen (14 procent) och reshjälpsappar med tidtabeller (13 procent).

Appar erbjuds ofta till låga eller inga kostnader och kan ha ett fåtal eller flera miljoner användare. I USA är i dag användning av en app det vanligaste sättet att få åtkomst till internet.[59]

Exempel på vilka slags personuppgifter som kan komma att hanteras i en app som laddas ner i en mobiltelefon är: användarens position, lagrade kontakter, unika identifieringsnummer för enheten, användarens namn, kreditkorts- och betalningsinformation, loggar över telefonsamtal och sms, webbläsarhistorik, användarens inlägg på sociala medier, e-post, bilder, videofilmer samt biometriska uppgifter (genom t.ex. ansiktsigenkänning och fingeravtryck).

Det bör dock noteras att alla appar inte begär åtkomst till samtliga ovanstående uppgifter. Det är också så att en app som begär åtkomst till uppgifter, inte nödvändigtvis skickar dessa vidare från telefonen.

Det är flera olika aktörer som kan ha möjlighet att ta del av uppgifter som samlas in från en smart enhet genom en app: apputvecklaren, appbutiken, operativsystemets tillverkare, enhetens tillverkare, företag som publicerar reklam i appen och företag som tillhandahåller analystjänster som hjälper apputvecklarna att ta reda på hur apparna används.

När den norska konsumentorganisationen Forbrukerrådet undersökte hur 20 populära appar (varav många är populära även i Sverige) hanterar uppgifter, var resultatet tydligt och oroväckande.[60] De flesta apparna kunde ändra användarvillkoren utan att förväg meddela kunderna på lämpligt sätt (med lämpligt sätt avses i undersökningen att på något aktivt sätt uppmärksamma kunderna på ändringarna, t.ex. genom att skicka ett mejl eller ha pop-up-fönster i tjänsten, dvs. inte bara att ändra villkoren på sin webbsida). Vissa appar hade otydliga definitioner av vad de anser vara personuppgifter och andra hade definitioner som inte är förenliga med dataskyddsbe-

[59] In the US, Time Spent With Mobile Apps Now Exceeds Desktop Web Access, http://www.marketingcharts.com/online/in-the-us-time-spent-with-mobile-apps-now-exceeds-the-desktop-web-41153/ Hämtat 2016-05-12.

[60] Rapporten *APPFAIL, Threats to Consumers in Mobile Apps*, Forbrukerrådet, mars 2016.

stämmelserna (dvs. att apparna hanterade personuppgifter som om det hade rört sig om uppgifter som inte går att härleda till enskilda personer). Överlag innehöll användarvillkoren många otydliga eller svåra begrepp. Elva av de granskade apparna begärde att få åtkomst till uppgifter som Forbrukerrådet menar inte rimligen kan behövas för den aktuella tjänsten. Ett flertal av apparna förbehöll sig rätten att anlita ospecificerade underleverantörer för sina tjänster, vilket enligt villkoren innefattade rätten att till dessa underleverantörer sprida uppgifter om kunderna. Forbrukerrådets granskning hittade även brister när det gällde bl.a. gallring (dvs. att uppgifter om kunderna kunde sparas för länge), möjligheten att ta tillbaka ett samtycke och diskrepanser mellan vad som sades i användarvillkoren och den faktiska hanteringen (t.ex. att uppgifter faktiskt lämnades ut till tredje part utan att detta nämndes i användarvillkoren eller att positionering gjordes även när appen inte var i bruk, vilket inte nämndes i användarvillkoren).

I Sverige har Råd & Rön[61] gjort en granskning av tolv populära löparappar avseende bl.a. hur användarnas personuppgifter skyddas.[62] I granskningen framkom bl.a. att det fanns brister i krypteringsskyddet (som skyddar mot avlyssning) vid överföring av uppgifter från apparna.

Organisationen Sveriges konsumenter anmälde i mars 2016 ett företag som ligger bakom en träningsapp till Konsumentverket för oskäliga avtalsvillkor och till Datainspektionen för att appens användarvillkor inte är förenliga med personuppgiftslagen. Organisationen grundar anmälan bl.a. på att användarvillkoren omfattar hela 38 sidor. Enligt Sveriges konsumenter kan det inte vara rimligt att förvänta sig att konsumenter ska läsa och sätta sig in i så omfattande användarvillkor när man skaffar sig något så trivialt som en träningsapp. Även innehållet i användarvillkoren ligger till grund för anmälan, bl.a. avseende rätten att sprida uppgifter till tredje part.

[61] Organisationen Sveriges konsumenters tidning.
[62] Malin Olsson (testansvarig Ronny Carlsson), *Bra funktion men dålig säkerhet*, publicerad i Råd & Rön nr 3 2016.

12.8.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter genom användning av appar. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

12.8.3 Risker för den personliga integriteten

Genom att appar samverkar så nära med operativsystemet får de åtkomst till betydligt mer uppgifter än en vanlig webbläsare. Apparna kan samla in och sprida stora mängder uppgifter från enheten och behandla dessa för att kunna erbjuda användaren olika tjänster.

En betydande risk med appar är bristen på information. Många appar informerar inte på ett meningsfullt sätt sina potentiella användare om vilken typ av personuppgifter appen kan behandla, i vilka syften och av vem. Bristen på öppenhet och insyn gäller inte bara gratisappar eller appar som tagits fram av oerfarna utvecklare.

Bristen på information hänger nära samman med en brist på informerat samtycke. När appen väl har laddats ned, ges samtycket vanligtvis bara genom att användaren får kryssa i en ruta för att godkänna villkoren, utan att det finns ett ”nej tack”-alternativ. Enligt en studie från september 2011 ville 92 procent av appanvändarna ha ett mer detaljerat val.[63]

Det finns också en risk för att bristfälliga säkerhetsåtgärder i apparna kan leda till otillåten hantering av personuppgifter, exempelvis om en apputvecklare råkar ut för dataintrång eller om själva appen läcker ut personuppgifter.

En annan risk är att personuppgifter som samlas in av appar kan spridas till ett antal tredjeparter och hos dessa användas för odefinierade eller mycket vida ändamål som exempelvis ”marknadsundersökning”.

Vidare förekommer inte sällan att appar samlar in mängder av uppgifter från telefonerna, utan att uppgifterna har något egentligt samband med appens funktion.

[63] Rapport från företaget Futuresight: *User perspectives on mobile privacy Summary of research findings*, september 2011.

12.9 Peer-to-peer-plattformar

12.9.1 Företeelsen

En ny företeelse på senare år, som snarare är av organisatorisk och affärsmässig natur än teknisk, är s.k. peer-to-peer-plattformar (inte att förväxla med peer-to-peer-nätverk som är en nätverksteknisk företeelse). Företeelsen är en del av delningsekonomins framväxt och är av intresse ur ett integritetsperspektiv, eftersom den bygger på tillgång till detaljerade och ständigt uppdaterade uppgiftssamlingar om både konsumenterna och om dem som utför tjänsterna.

Peer-to-peer-plattformar erbjuder plattformar för privatpersoner och företag att utbyta tjänster med varandra samt för att utvärdera och spåra dem som levererar med god kvalitet. Sådana plattformar av olika slag har funnits flera år, men börjar nu på allvar etablera sig som stora och seriösa aktörer. Två aktuella och omtalade exempel är Uber och AirBNB.

Plattformarna förlitar sig på data från sina kunder och leverantörer för att kunna tillhandahålla sina tjänster. I många fall är både kunder och leverantörer vanliga privatpersoner. Peer-to-peer-tjänsterna samlar därmed mycket information om enskilda personer.

Exempelvis kan en peer-to-peer-baserad tjänst för persontransporter gå ut på att sätta kunder i kontakt med förare med hjälp av en särskild app. I appen (dvs. hos företaget bakom tjänsten) hanteras alla nödvändiga data: resenärens och förarens identiteter, deras positioner, kreditkortsuppgifter och dylikt.[64]

12.9.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter i samband med peer-to-peer-plattformar. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om personuppgiftsansvar, ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

[64] Adam Erlandsson, *Uber vill starta priskrig i Stockholm*, publicerad den 29 januari 2014 på www.svd.se.

12.9.3 Risker för den personliga integriteten

Det finns en risk att företagen bakom tjänsterna använder personuppgifterna för nya ändamål, som kunden eller den som utövar en verksamhet inte har informerats om, som de inte har godkänt och som de inte heller hade kunnat föreställa sig då de ingick avtalet med företaget i fråga.

Enligt uppgifter i media ska det exempelvis ha inträffat att peer-to-peer-företag använt uppgifter för att tysta kritiska journalister, för att bedriva egna undersökningar på kundddata och förevisa kunddata som underhållning på personalfester.[65] Efter den mediala uppmärksamheten har det aktuella företaget uppgett att man åtgärdat problemen.[66]

Även om sådan användning är extrem och knappast är representativ för branschen, illustrerar exemplet ändå på ett tydligt sätt vad som faktiskt kan hända.

12.10 Kommitténs samlade bedömning av området

De senare årens teknikutveckling i kombination med nya användningsområden och nya vanor, har inneburit att det genereras allt mer data om våra konsumtionsrelaterade beteenden.

Det är en allt mindre del av all data i världen som skrivs in eller på annat sätt medvetet genereras direkt av användarna. Mer och mer data genereras i stället rent maskinellt, utan mänsklig inblandning.

Utvecklingen har också inneburit att alla dessa uppgifter i större utsträckning faktiskt går att bearbeta och analysera samlat i realtid.

Den här utvecklingen kan självklart vara till nytta för den enskilde konsumenten på många sätt, men möjliggör samtidigt en allt mer omfattande kartläggning på individnivå. Kartläggningen ökar både på bredden och på djupet genom att fler och nya slags uppgifter samlas in och samkörs.

Ett grundläggande problem är att enskilda användare – trots ett i många delar tydligt regelverk – inte informeras om den ökande hanteringen på ett heltäckande men ändå lättfattligt sätt. Därtill kommer

[65] Craig Timberg, *Is Uber's rider database a sitting duck for hackers?*, publicerad den 1 december 2014 på www.washingtonpost.com.
[66] Sam Frizell, *What Uber Still Won't Say About Your Data*, publicerad den 30 januari 2015 på www.time.com.

att det rent allmänt finns en relativt låg medvetenhet i befolkningen om hur vardagsgöromål som inte uppfattas som ett uppgiftslämnande, faktiskt genererar elektroniska spår och hur dessa spår samlas in, sparas och används. Det finns inte heller någon större medvetenhet om att personuppgifter faktiskt är en värdefull handelsvara, särskilt i tjänster som marknadsförs som ”gratis”.

Ett annat grundläggande problem är att uppgifter i allt större utsträckning börjar användas för andra ändamål än dem för vilka de ursprungligen samlades in, vilket brukar kallas för ”ändamålsglidning”. Det är inte förenligt med personuppgiftslagen, om det nya ändamålet är oförenligt med det ursprungliga. När ett stort antal i sig harmlösa uppgifter från olika sammanhang bearbetas och analyseras samlat, kan de tillsammans ge nya och tidigare oanade kunskaper om enskildas personligheter och användas för att göra antaganden om deras framtida beteende. Dessa nya kunskaper kan i sin tur väcka intresse för uppgifterna hos aktörer som exempelvis försäkringsbolag och kreditgivare.

Frågan om ändamålet med en hantering är nära förknippad med frågan om de samtycken som enskilda lämnar i olika sammanhang. Det sägs ibland vara den vanligaste lögnen på internet att svara *ja* på frågan om man läst och förstått företagets (dvs. webbplatsens, kundklubbens, betalningsföretagets, appleverantörens) användarvillkor och därmed samtyckt till hur ens personuppgifter kommer hanteras.[67] De långa och invecklade användarvillkoren kan vara i stort sett omöjliga att förstå för gemene man, och särskilt för barn eller personer som har en funktionsnedsättning.

En viktig faktor i sammanhanget är de inblandade aktörernas intresse att samla in så mycket data som möjligt om användarna. Det finns i dag en allmänt spridd och mycket stark tro på att även data som i dagsläget egentligen inte kan användas på något vettigt sätt, i en snar framtid kan förvandlas till avgörande tillgångar, både rent affärsmässigt och för att lösa svåra problem i samhället. Det har uppstått nya affärsmodeller och nya aktörer som har personuppgifter som främsta eller enda handelsvara, som exempelvis datamäklare.

[67] En studie från år 2008 visade att en genomsnittlig användare skulle behöva 244 timmar för att läsa igenom samtliga användarvillkor för de sajter hon eller han besökte under loppet av ett år. I USA har presidentens vetenskaps- och teknologiråd sammanfattat situationen med att det bara är i en fantasivärld som enskilda faktiskt läser och förstår villkoren och klickar i att de samtycker.

Intresset av att samla in så stora mängder uppgifter som möjligt är således mycket starkt. Det framstår därmed inte som sannolikt att aktörerna eller marknaden på eget initiativ skulle begränsa kartläggningen av konsumenter och ge enskilda reell insyn i hur deras uppgifter hanteras och ge dem möjlighet att påverka hanteringen.

En annan risk för konsumenter avser informationssäkerhet. Som framgått av detta avsnitt är det inte alltid som nya teknikanvändningar möjliggör ett tillräckligt starkt skydd för personuppgifterna.

Det finns emellertid vissa tecken på att allmänheten i samband med Edward Snowdens avslöjanden kan ha blivit något mer medveten när det gäller informationssäkerhetsfrågor och skyddet för de egna personuppgifterna i olika webbtjänster. Avslöjandena har även föranlett många tjänsteleverantörer att förbättra skyddet i sina tjänster genom att exempelvis införa kryptering som bara kunden har nyckeln till.[68]

Men även om det finns enstaka, lovvärda initiativ från aktörerna till att stärka integritetsskyddet för konsumenter, är dessa inte tillräckliga om man betraktar den pågående utvecklingen i sin helhet. Det krävs mer systemövergripande och grundläggande åtgärder för att stärka skyddet – redan i dag och ännu mer i en snar framtid.

Det kan också konstateras att flertalet företeelser som nämns i det här kapitlet inte har granskats ur ett integritetsskyddsperspektiv på senare år. De granskningar som görs av Post- och telestyrelsen (kakor) och av Datainspektionen (elektroniska betalningar och WiFi-tracking) är tillsynsaktiviteter riktade mot vissa specifika aktörer.

Konsumentverket omnämner i sin omvärldsrapport för år 2014 digitaliseringens påverkan på konsumenternas ställning, men har därutöver hittills inte varit aktivt när det gäller integritetsskyddsfrågor, t.ex. beträffande frågor om de sociala mediernas avtalsvillkor om personuppgifter.[69]

Det finns således i dagsläget ingen myndighet eller organisation som har en uppdaterad och allmän överblick över vilka företeelser som innebär risker för konsumenter, hur spridda företeelserna är, vilka aktörer de används av osv. och som därmed kan sägas ha en överblick över utvecklingen för konsumenters personliga integritet.

[68] Norska Teknologirådets och Datatilsynets gemensamma rapport *Personvern 2015 – tillstand og trender*, januari 2015.

[69] Konsumentverkets rapport 2014:13, *Vår omvärld 2014 – rapport till regeringen 2014-11-30*.

En tillkommande risk är att alla uppgifter som genereras av sakernas internet, kan komma att begäras in av olika företag, som exempelvis försäkringsbolag. När de många och detaljerade uppgifterna väl finns, kommer de att attrahera många olika intressenter.

Det är redan i dag mycket svårt att som konsument använda sig av digitaliseringens och teknikutvecklingens alla fördelar utan att, mer eller mindre ofrivilligt, kartläggas på en detaljerad nivå. Det finns en överhängande risk för att det i framtiden kommer att bli ännu svårare.

Bristen på information, samtyckets urholkning, den stora spridningen av uppgifter för nya ändamål och den ökade totala mängden av uppgifter om den enskilde, innebär att kommittén sammantaget anser att det finns allvarliga risker för konsumenters personliga integritet.

Samtidigt måste beaktas att utvecklingen för med sig stora fördelar för den enskilde konsumenten, exempelvis i form av nya tjänster, ökad tillgång till produkter samt större möjlighet till delaktighet och till att själv skapa tjänster och produkter. Utvecklingen visar också vissa tecken på att enskilda blivit mer medvetna och bättre på att tillvarata de möjligheter som faktiskt finns att vidta egna åtgärder för att skydda sin personliga integritet.

13 Sociala medier och e-post

Kommitténs bedömning: Användning av vissa sociala medier innebär en allvarlig risk för den personliga integriteten.

Användning av e-post innebär en påtaglig risk för den personliga integriteten.

13.1 Sociala medier

13.1.1 Avgränsning

Sociala medier som företeelse har redan berörts i kapitlen om skolan, arbetsliv och konsumentområdet. Myndigheters användning av sociala medier behandlas i kapitel 11 om e-förvaltning.

I det här kapitlet behandlas de övergripande egenskaperna hos sociala medier. Kapitlet tar i huvudsak upp hantering av uppgifter hos företag och organisationer som tillhandahåller olika slags sociala medier. Även hur enskilda personer med hjälp av sociala medier hanterar uppgifter om andra personer, behandlas till viss del. Emellertid berörs inte den straffrättsliga aspekten av enskildas hantering av personuppgifter i sociala medier, eftersom den frågan nyligen behandlats av Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten. Utredningen lämnade i februari 2016 betänkandet *Integritet och straffskydd*.[1]

Även avsnitt 21.1 om molntjänster är av relevans när det gäller den personliga integriteten i sociala medier, eftersom sociala medier i allmänhet bygger på olika slags molntjänster.

[1] Utredningens om ett modernt och starkt straffrättsligt skydd för den personliga integriteten betänkande *Integritet och straffskydd*, SOU 2016:7.

13.1.2 Begreppet sociala medier

Begreppet sociala medier används för att särskilja en relativt ny typ av nätbaserade tjänster från det som ibland kallas för traditionella medier. I traditionella medier finns en tydlig avsändare och en stor publik. I de sociala medierna har alla användare möjlighet att själva välja vilken roll de vill ha, och att växla mellan rollerna. Ena stunden skriver användaren en text eller spelar in en film som han eller hon delar med sina vänner, i nästa stund kommenterar användaren en statusuppdatering eller ett foto som en bekant har publicerat. Andra gånger är användaren mer passiv och läser, tittar och lyssnat utan att själv bidra med något innehåll.

Spännvidden i de sociala medierna är stor. Till kategorin kan man bland annat räkna bloggar, diskussionsforum och artikelkommentarer. Även många on-line-spel innehåller diskussionsforum eller chattar som ger dem karaktär av sociala medier. Till de sociala medierna räknas givetvis den typ av tjänster som brukar benämnas som sociala nätverkssajter. Till den sistnämnda kategorin hör bland annat tjänster som Facebook, Twitter, Instagram, Kik, Ask och Periscope. I detta kapitel används beteckningen sociala medier i bred bemärkelse, som ett samlingsbegrepp för de olika former av sociala medier som finns i dag. Beteckningen används här såväl för de sociala medierna i sig, som för de företag som tillhandahåller de sociala medierna.

Användningen av sociala medier bland befolkningen undersöks med jämna mellanrum. Det visar sig då att användningen varierar beroende på bl.a. ålder och kön. Exempelvis är sociala nätverkssajter något mer populära bland flickor i åldern 11–16 år, jämfört med pojkar i samma ålder vilka gärna ägnar sig åt spel på nätet, vilket i sin tur inte alls är lika populärt bland flickor i samma åldersgrupp.[2]

I en annan rapport finns generella siffror om användningen av sociala medier.[3] Enligt denna undersökning är Facebook fortfarande det sociala nätverk som dominerar. Hela 70 procent av internetanvändarna använder Facebook åtminstone någon gång och nästan alla som besöker sociala nätverk besöker också Facebook. Bildbaserade nätverk får allt större spridning, särskilt bland de unga. Instagram ökar mest, totalt 40 procent av internetanvändarna använder nu

[2] Rapport från Internetstiftelsen i Sverige, *Eleverna och internet 2015*, av Kristina Alexanderson och Pamela Davidsson.

[3] Rapport från Internetstiftelsen i Sverige, *Svenskarna och internet – 2015 års undersökning av svenska folkets internetvanor*, av Olle Findahl och Pamela Davidsson.

tjänsten. Snapchat används däremot främst av tonåringar. Både Twitter och LinkedIn används av en av fem internetanvändare. Men ännu är det traditionell e-post och korta snabbmeddelanden som dominerar den dagliga kommunikationen på internet.

Sett över alla åldrar är kvinnor mer aktiva än män när det gäller att kommunicera över internet och besöka sociala medier.[4] Det gäller framför allt i den dagliga användningen. Skillnaderna är särskilt stora vad gäller dagliga besök på Instagram (22 procent av kvinnorna respektive 12 procent av männen), Facebook (53 procent respektive 41 procent), bloggar (13 procent respektive 5 procent), SMS (60 procent respektive 50 procent) och dagliga besök på sociala medier med mobilen (65 procent respektive 48 procent). Det är också något vanligare att kvinnor publicerar var de befinner sig (21 procent respektive 13 procent minst någon gång i veckan). Siffrorna avser procent av den del av befolkningen tillhörande respektive kön som över huvud taget använder sig av internet. Men det föreligger inga stora skillnader mellan män och kvinnor i hur ofta de använder e-post, Twitter, Instant messaging, besöker chattrum eller skickar mms.

Att utvecklingen och användningen av sociala medier formligen har exploderat de senaste åren är närmast en truism. Siffrorna som anger hur mycket data som användare lägger ut på sociala medier varierar, men är alltid mer eller mindre svindlande. Exempelvis har ett it-företag gjort beräkningar som visar att det under år 2014 *varje minut* delades innehåll 2,5 miljoner gånger på Facebook, tweetades 300 000 gånger, postades 220 000 nya bilder på Instagram och lades upp 72 timmar nytt videoinnehåll på Youtube.

När det kommer till att använda denna enorma datamassa är uppfinningsrikedomen mycket stor och på ständig frammarsch. Bara som ett exempel rapporterades under år 2015 att Google försöker utveckla en teknik för att utifrån bilder på maträtter kunna utläsa hur många kalorier dessa innehåller, vilket ska ses mot bakgrund av att de flesta bilder i sociala medier går att härleda till enskilda individer.[5]

Till utseende och funktion skiljer de olika tjänsterna sig åt, men många funktioner återkommer, däribland dessa:

– möjlighet finns att skapa ett eget lösenordskyddat konto,

[4] Rapport från Internetstiftelsen i Sverige, *Svenskarna och internet 2014*, av Olle Findahl.
[5] Jon Fingas, *Google hopes to count the calories in your food photos*, publicerad den 2 juni 2015 på www.engadget.com.

– möjlighet finns att leta upp vänner och bekanta och lägga till dem på en kontaktlista för att underlätta kontakten med dem,
– möjlighet finns att skapa eller ladda upp eget material. Det kan vara korta statusuppdateringar eller längre texter, det kan vara bilder och filmsekvenser, det kan vara ljud eller annat,
– möjlighet finns att göra inställningar som styr vilka andra personer som kan se det som laddas upp,
– möjlighet finns att se innehåll som andra användare har skapat, att lämna kommentarer eller på andra sätt interagera och ibland även dela med andra användare.

Det finns studier som gör gällande att användningen av sociala medier är starkt beroendeframkallande.[6] Beroendet har beskrivits på följande sätt:

> Sociala medier erbjuder inget innehåll. Det är vi själva som är innehållet. Därför gäller det att hela tiden upprätthålla vårt intresse, vår närvaro. Helst skall vi logga in flera gånger varje dag, helst skall vi uppdatera, gilla och sprida bilder, texter och tankar mest hela tiden, annars riskerar affärsmodellen att kollapsa. Därför, påpekar Christian Fuchs, är sociala medier konstruerade för att upprätthålla vårt intresse. De kopplar upp sig mot våra mest basala känslor och behov, de levererar en plattform som gör att vi känner oss uppskattade, populära och intressanta. De är medvetet konstruerade för att vi skall få en positiv kick.[7]

13.1.3 Olika kategorier av sociala medier

Sociala medier kan delas in och kategoriseras på många olika sätt. Indelningen och beskrivningen som följer här, är i allt väsentligt hämtad från Statens medieråds beskrivning av sociala medier såsom den återges i betänkandet *Integritet och straffskydd*.[8]

Vissa sociala medier är särskilt utformade för visuell kommunikation, exempelvis bilddelningstjänster som Instagram, eller videodelningsplattformar som YouTube. Andra är utformade för snabb, främst textbaserad kommunikation, som exempelvis Twitter och

[6] Johan Åkesson, *Uppdaterade och sömnlösa*, publicerad den 14 februari 2012 på www.dn.se.
[7] Mattias Hagberg, *Gilla på egen risk*, publicerad den 20 juni 2013 på www.gp.se
[8] SOU 2016:7.

KiK. I vissa sociala medier sker kommunikationen flyktigt i avgränsade grupper (i chatappar som exempelvis Snapchat), i andra handlar det om en mer beständig kommunikation i identitetsbaserade sociala nätverk som exempelvis Facebook. Flera sociala medier kan också kopplas till traditionella medier. Exempelvis använder sig flera tidningars webbupplagor av en koppling mot sociala medier (t.ex. Facebook) som kommentarsfält i stället för att ha en egen kommentarsfunktion på sajten. På diskussionsforum som t.ex. Flashback och Familjeliv kan användare samtala om i princip allt i en enorm mängd diskussionstrådar. Denna typ av forum har också en mycket varierande grad av moderering, med bl.a. den effekten att de låter användarna publicera omfattande samlingar av uppgifter om andra personer, vilka ibland kan vara synnerligen ovälkomna, närgångna och kränkande för de omtalade personerna.

En viktig aspekt av den förändring som sociala medier genomgått under de senaste åren, är kopplingen till det fysiska rummet. Tidigare var sociala medier anpassade till stationära eller bärbara datorer genom uppkoppling via webben, men är nu anpassade för att användas i mobiltelefonen. Vissa sociala medier existerar inte ens på webben utan går enbart att använda genom en app i en smart mobiltelefon. De sociala mediernas ökade mobilitet innebär att man snabbare och enklare kan lägga upp information än tidigare. Förr behövde man ta en bild och sedan föra över den till en dator innan man kunde lägga upp den på Facebook. I dag sköts allt omedelbart i en smart mobiltelefon.

I dag finns det många tekniska möjligheter för användaren att sammanlänka olika sociala medier, exempelvis genom att delning av information görs automatiskt på flera plattformar. Det är möjligt att ta en bild med mobiltelefonen, dela den på t.ex. Instagram, som kopplats till Facebook och till en blogg. På så sätt så görs delningen samtidigt på dessa tre plattformar. Begränsningen i delningen per plattform beror på hur man som användare konfigurerat delningarna. Sociala plattformar kan också användas som inloggningsnyckel till andra tjänster och applikationer. I stället för att skapa nya konton till alla nya tjänster, kan man exempelvis välja att logga i med sitt Facebook-konto. Många sociala medier möjliggör användaranonymitet, dvs. identifierbara uppgifter hålls hemliga av den som äger tjänsten. Exempelvis är Twitter en sådan plattform – här väljer användaren själv om kontot ska vara identifierbart till en person. Det finns

även tjänster vars affärsmodell är att tillhandahålla användarna fullständig anonymitet. Vissa av dessa innebär också att användaren kan vara anonym i relation till den som tillhandahåller tjänster, t.ex. Cloaq.

13.1.4 Funktioner för klagomålshantering

Många sociala medier tillhandahåller ett kontaktformulär som personer kan använda sig av om de har klagomål på sådant som publicerats på det sociala mediet, exempelvis när någon användare har publicerat kränkande inlägg.

Datainspektionen har tagit fram en särskild webbplats, www.krankt.se, som riktar sig till barn och ungdomar, där det finns en lista med kontaktuppgifter till de vanligaste sociala mediernas sidor för klagomålshantering.

Det är svårt att bilda sig en överblick över vilka slags klagomål som riktas till de sociala medierna och hur dessa hanterar klagomålen. I en granskning från år 2014 av hanteringen av enskildas klagomål med anledning av kränkningar av kvinnor på Facebook, Twitter och Youtube, riktades kritik bl.a. mot att dessa sociala medier inte självmant arbetade med att förbättra sin hantering av sådana klagomål, utan att detta gjordes först när det hade inträffat kränkningar som blivit medialt uppmärksammade. De sociala medierna kritiserades också för att inte tillräckligt tydligt berätta för dem som vill anmäla kränkningar hur klagomålen skulle hanteras av det sociala mediet.[9]

Under vintern 2016 har svenska media beskrivit de stora svårigheterna med att förmå i synnerhet Facebook att ta bort material som kan anses som hatiskt och hotfullt mot vissa namngivna personer.[10]

[9] Rapporten *End violence: Women's rights and safety online Internet intermediaries and violence against women online, Executive summary and findings*, publicerad i juli 2014 av Association for Progressive Communications.

[10] Se t.ex. Jack Werner, *Hatet som Facebook vägrar att ta bort*, publicerad i Svenska dagbladet den 29 februari 2016.

13.1.5 Annonsförsäljning

Av betydelse i sammanhanget är att de flesta sociala medierna är gratis för användarna. I den mån de genererar några intäkter kommer dessa i huvudsak från annonsförsäljning, men det förekommer även tjänster som under många år finansieras av riskkapitalbolag där förhoppningen är att längre fram i tjänstens utveckling hitta en fungerande intäktsmodell.

För att bli en attraktiv plattform för annonsörer finns det två vägar att gå, vilka inte sällan kombineras. Dels handlar det om volym, dvs. att tjänsten har många användare som annonsörerna kan nå. Dels handlar det om kvalitet, dvs. att tjänsten kan erbjuda annonsörerna rätt publik. I traditionella medier görs ofta publikundersökningar för att få reda på vilka som läser, tittar eller lyssnar på mediet i fråga. I enkäter ställs då frågor om ålder, kön, inkomst, intressen och så vidare. Med den informationen går det att ta fram en profil över en typisk konsument av det aktuella mediet. Till annonsörerna kan det sedan riktas ett erbjudande om att nå dessa typiska konsumenter.

Sociala medier öppnar helt nya möjligheter för riktad reklam, med hjälp av all den information som användarna lämnar ifrån sig i kombination med den information som skapas om dem.

Den kunskap som företagen bakom de sociala medierna har om sina användare används inte bara i reklamsyfte. Samma information används också för att utveckla tjänsten vidare. Företagen kan se vad användarna uppskattar respektive vad de ogillar, och kan anpassa den fortsatta utvecklingen av tjänsterna efter detta.

Det har på senare tid blivit allt vanligare att enskilda på olika sätt väljer bort reklam på nätet, exempelvis genom att installera en s.k. adblocker som är ett tillägg i webbläsaren som blockerar annonser på webbsidor.

13.1.6 Två typer av information

I de sociala medierna finns i huvudsak två typer av information. Det handlar dels om information som användarna själva skapar och dels om information som företagen bakom tjänsterna skapar om sina användare med hjälp av sambearbetningar av olika datakällor, såväl egna som externa.

Användarna är i allmänhet medvetna om de sprider information till andra användare. Däremot förstår de inte alltid vilka personer som faktiskt kan se deras innehåll.

Det är ofta oklart hur tjänsternas integritetsinställningar fungerar. När en grupp forskare år 2011 undersökte i vilken utsträckning användare förstod integritetsinställningarna hos Facebook, kunde de konstatera att av de undersökta exemplen hade bara 37 procent av statusuppdateringarna och bilderna de integritetsinställningar som var användarens avsikt.[11] I majoriteten av fallen där de faktiska inställningarna och användarnas avsikt inte stämde överrens, visades innehållet för fler än det var tänkt. Av 907 slumpvist utvalda bilder från 197 Facebook-användare, var hälften tillgängliga för vem som helst, tvärt emot vad som var användarnas avsikt.

En annan svårighet för användarna är de tredjepartsapplikationer som går att installera i ett Facebook-konto. Typiska exempel på tredjepartsapplikationer på Facebook är spel och olika typer av tester där användaren svarar på frågor. När en användare installerar en ny Facebook-app dyker det upp en ruta där man ser vilka rättigheter appen i fråga behöver. Problemet är att man många gånger inte bara ger appen tillgång till information om sig själv, utan även information om sina vänner. Bland de integritetsinställningar som Facebooks användare kan göra finns möjligheten att begränsa vilken information som tillgängliggörs för de appar som vännerna använder sig av. Men standardinställningen tillåter en bred och omfattande åtkomst till många olika slags uppgifter. För en nybliven användare på Facebook fick i maj 2015 vännernas appar bland annat tillgång till statusuppdateringar, familjerelationer, utbildning och arbetsgivare. Användarvillkor och användningen ändras kontinuerligt för de flesta sociala medier, och detaljerade beskrivningar blir därför snabbt inaktuella.

Vid sidan av den information som användarna själva medvetet skapar eller laddar upp till de sociala medierna, skapas också en hel del information om dem. Med hjälp av kakor (på engelska cookies), små textfiler som sparas i webbläsaren, går det till exempel att följa vilka webbplatser som besöks. I takt med att Facebook har växt har andra webbplatser sett fördelar med att lägga till Facebookfunktioner,

[11] Yabing Liu m.fl., *Analyzing Facebook Privacy Settings: User Expectations vs. Reality* – i Proceedings of the 11th ACM/USENIX Internet Measurement Conference (IMC'11), Berlin, 2011.

som gilla-knappar och kommentarsfält. För webbplatserna blir detta ett enkelt sätt att lägga till sociala funktioner och samtidigt få ökad spridning. Men det innebär också att Facebook får information om vilka sidor enskilda användare besöker på webben. Detta gäller oavsett om besökaren på en webbsida trycker på gilla-knappen eller inte. Varje gång en sida med en sådan knapp laddas i en webbläsare hämtas knappen från Facebooks servrar, varvid Facebook får veta vilken användare det handlar om. Ett klick på knappen ger dock mer information, eftersom det även talar om att innehållet är något som användaren gillar.

Kakor och gilla-knappar är långt ifrån de enda sätten att registrera en användares beteende. Pixelspårning och digitala fingeravtryck är två andra exempel. Pixelspårning har till sin funktion mycket gemensamt med de gilla-knappar som finns på andra webbplatser än Facebook. Genom att lägga in en väldigt liten och genomskinlig bild förändras inte användarens upplevelse av webbsidan, men eftersom adressen till bilden är unik för varje användare går det att veta vem som besökt sidan. Digitala fingeravtryck har behandlats i kapitel 12 om konsumentområdet.

Den belgiska dataskyddsmyndigheten publicerade i maj 2015 en rapport om Facebooks kartläggning av enskildas surfvanor. I rapporten konstaterar myndigheten bland annat att Facebook spårar alla som kommer in på sidor som har ett av företagets sociala insticksprogram (på engelska *social plug-in*). Exempel på sådana är Facebooks knappar för att ”gilla” eller ”dela” vilka finns på många webbsidor utanför Facebooks egen domän. Den belgiska myndigheten beskriver hur Facebook placerar en unik kaka på användarens dator vid besök på en sida som har en av Facebooks knappar för sociala insticksprogram. Med hjälp av den unika kakan registrerar sedan Facebook användarens alla besök på andra sidor som också har en av Facebooks knappar, även om användaren saknar konto hos Facebook. Myndigheten rekommenderar i rapporten bl.a. att Facebook ska sluta upp med att utan samtycke placera kakor hos och spåra användare som inte själva har ett konto hos Facebook.[12]

[12] Commissie voor de bescherming van de persoonlijke levenssfeer, Rekommendation nr 04/2015 av den 13 maj 2015.

En belgisk domstol har i november 2015 förelagt Facebook att sluta spåra användare som saknar egna konton hos Facebook.[13] Domstolen beslutade även att Facebook skulle betala 250 000 euro per dag så länge Facebook inte inrättar sig efter domstolens föreläggande.

Tillsynen av hanteringen av personuppgifter i sociala medier har i Sverige huvudsakligen varit inriktad på hur användare, både enskilda individer och företag eller myndigheter, hanterar uppgifter om andra personer. Endast i ett fåtal fall har de som tillhandahåller sociala medier granskats. Vissa globala medier som exempelvis Facebook, hanteras gemensamt i Artikel 29-gruppen, även om några nationella tillsynsmyndigheter inom EU på eget initiativ granskat just Facebooks hantering av uppgifter om det egna landets invånare.

13.1.7 Vilka har intresse för uppgifter om användarna?

I sociala medier finns således stora mängder information om användarna. Denna informationsmängd är av potentiellt intresse för många olika parter. Det saknas tillförlitlig, svensk statistik över omfattningen av hur många personuppgifter som varje år läcker från svenska organisationer och myndigheter. Siffror från USA ger vid handen att antalet läckta uppgifter pga. antagonistiska attacker (på engelska hacking/skimming/phising) har ökat radikalt under de senaste åren.[14]

Företag

Från näringslivet är intresset för användarnas information sprunget ur dess kommersiella potential. De stora sociala medierna är uteslutande gratis för användarna och finansieras i stället av annonsintäkter. Genom att ha stora mängder information om sina användare går det att erbjuda annonsörerna att göra snäva urval för sina reklamkampanjer. Jämfört med traditionella medier, där kunskapen om en viss tidnings läsare eller en viss tv-kanals tittare är relativt grovhuggen,

[13] Beslut den 9 november 2015 av Nederlandstalige rechtbank van eerste aanleg Brussel i mål nr 15/57/C.

[14] Identity Theft Resource Center Breach Report Hits Near Record High in 2015. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html Hämtat 2016-05-10.

kan sociala medier låta annonsörerna göra betydligt mer finmaskiga urval, baserade på bland annat bostadsort, kön, ålder, civilstånd, intressen och så vidare. Ju bättre sorteringsmöjligheter, desto träffsäkrare annonskampanjer vilket i sin tur leder till ett bättre erbjudande till annonsmarknaden.

Det går att förbättra möjligheterna ytterligare, genom att inkludera uppgifter från inköp gjorda i fysiska butiker. Exempelvis har Facebook samarbeten med Datalogix, Epsilon, Acxiom och BlueKai. Alla fyra företagen samlar in stora datamängder, från bland annat amerikanska butikskedjors bonusprogram. Annonsörer kan sedan välja att visa reklam för befintliga kunder. Facebook erbjuder också möjligheten att rikta annonser till personer som finns med i en befintlig databas och matcha dem mot användare på Facebook med hjälp av exempelvis telefonnummer eller e-postadress. Det går också att först använda pixelspårning för att se vilka Facebook-användare som besöker en viss webbplats och sen välja att visa annonser bara för dem.

För företagen som tillhandahåller de sociala medierna finns det också andra anledningar att känna till så mycket som möjligt om sina användare. Genom att ha kunskap om sina användare ökar möjligheterna att bygga en tjänst som intresserar dem och som de återkommer till, helst många gånger varje dag. Därmed ökar företagen som tillhandahåller de sociala medierna ytterligare sitt värde som annonsmarknad.

De sociala medierna kan dock även ha andra intressen än annonsförsäljning när det gäller användarnas personuppgifter. Internetstiftelsen i Sverige nämner i en av sina informationsskrifter att Facebook i början av år 2012 gjorde en undersökning på nästan 690 000 användare i flera olika länder utan deras vetskap. Syftet med undersökningen var att ta reda på hur människor reagerar på positiva respektive negativa kommentarer. Under en vecka fick försökspersonerna se antingen övervägande positiva eller övervägande negativa kommentarer i sina flöden på Facebook. Resultatet visade att tonen i statusuppdateringarna smittade: de som såg positiva kommentarer skrev också själva mer positiva inlägg. Den aktuella undersökningen var förenlig med Facebooks då rådande policy, enligt vilken uppgifter

om användarna kunde användas ”för interna åtgärder, däribland felsökning, dataanalys, testning, forskning, utveckling och tjänsteförbättring”.[15]

Intressebaserad kartläggning av organisationer

Det är inte bara företag med produkter och tjänster att sälja som är intresserade av att utnyttja informationen i sociala medierna i marknadsföringssyfte. Samma möjligheter lockar även organisationer som vill nå ut med sitt budskap. Det kan till exempel handla om politiska partier.

Precis som näringslivet kan politiska organisationer gå från masskommunikation i form av bland annat valaffischer på anslagstavlor och tidningsannonser till helt personanpassad kommunikation. I detta sammanhang brukar Barack Obamas omvalskampanj år 2012 nämnas som särskilt innovativ. Bl.a. använde man sig av data från ett flertal olika källor för att beräkna sannolikheten för valdeltagande ner på individnivå, vilket gjorde det möjligt att rikta kampanjinsatserna till personer där de skulle ge bäst utdelning.[16]

Informationsstölder av hackare

Sociala medier som lagrar stora informationsmängder blir självklart också måltavlor för kriminell verksamhet. Syftet kan vara att leta material i utpressningssyfte, att använda ett kapat konto för bedrägerier eller komma över kontokortsuppgifter för att sälja dessa på svarta marknaden.

Underrättelsetjänster

Svenska brottsbekämpande myndigheters möjligheter att få åtkomst till uppgifter i sociala medier behandlas i kapitel 18.

---

[15] Internetstiftelsens i Sverige internetguide nr 35, *Användarvillkoren som ingen läser*, version 1.0, 2015, författad av Johanna Lundeberg.

[16] Zeynep Tufekci, *Engineering the Public: Big Data, Surveillance and Computational Politics*, First Monday, Volume 19, Number 7, July 2014.

Mycket av de senaste årens debatt om personlig integritet har handlat om amerikanska myndigheters massövervakning av vad egna och andra länders medborgares gör på nätet. Debatten inleddes under sommaren 2013 när Edward Snowden började avslöja hemligstämplade dokument om USA:s massövervakning till journalisterna Glenn Greenwald och Laura Poitras. Den därmed avslöjade övervakningen har ändrat synen på vilket integritetsskydd som ges i USA för uppgifter om EU-medborgare (se nedan om det skyddande regelverket).

13.1.8 Radering av uppgifter i sociala medier

Det är i praktiken omöjligt för användare av sociala medier att ha någon insyn i hur och var de egna uppgifterna lagras. Uppgifterna finns ofta utspridda över flera servrar runt om i världen, och har dessutom sannolikt säkerhetskopierats på ytterligare några platser. Det här får konsekvenser den dag en användare vill radera en bild som användaren publicerat i det sociala mediet. För användaren och dennes vänner försvinner ofta bilden eller videosekvensen omgående. Men innan den även försvunnit från alla företagets servrar kan det gå längre tid, under vilken den som har en direktadress till innehållet fortfarande kan komma åt bilden.

Beroende på hur tjänsteleverantören löst säkerhetskopieringen av användarnas data kan det dessutom vara så att det är mer kostnadseffektivt för företaget att inte radera bilden eller filmen ur alla säkerhetskopior. För användaren ser det alltså ut som om det material som inte längre var önskvärt att ha publicerat på nätet är raderat. Det stämmer också så till vida att varken användaren eller dennes vänner längre kan komma åt det som en gång publicerades. Men materialet kan ändå finnas kvar hos det sociala mediet.

13.1.9 Användarvillkor

Användarvillkoren hos de sociala medierna varierar i omfång och begriplighet. De är oftast långa och invecklade och kan vara otydliga på en del viktiga punkter, t.ex. hur uppgifterna får vidareanvändas och spridas till det sociala mediets samarbetsparter. När en användare

skapar ett nytt konto hos något av nätets sociala medier visas vanligtvis användarvillkoren upp, och användaren måste bekräfta att de är lästa genom att kryssa i en ruta.

Användarvillkor av varierande komplexitet i kombination med användarnas ointresse av att läsa dem är problematiskt. Många användare känner inte till villkoren som de har accepterat och även om de skulle läsa dem, är det inte enkelt att förstå vilken information som samlas in och hur den faktiskt används.

Det finns organisationer som försöker hjälpa enskilda att få en enkel överblick över vilka villkor som gäller för bl.a. olika sociala medier. Exempelvis finns webplatsen tosback.org som har som målsättning att komma till rätta med vad den anser vara den största lögnen på nätet, vilket är uttalandet ”jag har läst och godkänt användarvillkoren”. På webbplatsen listas sammanfattningar och aktuella förändringar av de större företagens användarvillkor. Av sammanfattningarna framgår att det är vanligt med användarvillkor som ger respektive företag en vidsträckt rätt att vidareanvända och sprida uppgifter om användarna utanför den egna organisationen. Det förekommer också att användarvillkoren föreskriver att tvister ska prövas enligt gällande rätt i någon av USA:s delstater, och att användarna avstår från att exempelvis medverka i en grupptalan mot det sociala mediet.

13.2 E-post

E-post, även kallat mejl, är en sätt att skicka meddelanden från en avsändare till en eller flera mottagare över nätet. I detta kapitel används begreppen e-post och mejl omväxlande och i allt väsentligt som synonymer.

Ett e-postmeddelande förmedlas vanligen med hjälp av nätverksprotokollet SMTP (Simple Mail Transfer Protocol) via ett antal serverdatorer. E-posten läses med ett klientprogram som antingen kommer åt e-posten som filer på datorn eller kommunicerar med en mejlserver.

Webbmejl är webbaserade system som ger användaren möjlighet att läsa och skriva e-post med en vanlig webbläsare i stället för med en särskild e-postklient.[17]

[17] ”Webbpost.” Wikipedia, https://sv.wikipedia.org/wiki/Webbpost Hämtat 2016-05-10.

Många universitet och skolor använder webbmejl för att ge studenter och personal webbaserad åtkomst till sina mejlkonton och andra relaterade tjänster som personlig kalender, anteckningar och att göra-listor. Dessutom erbjuder de flesta internetleverantörer access till sina mejltjänster via webben. Det finns också fristående webbmejltjänster.

Programvaran för webbmejl kommunicerar ofta med en normal mejlserver som sköter mottagning, lagring och filtrering av inkommande post och kontroll, lagring och sändning av utgående post, och med en normal webbserver för kommunikation med webbläsaren. Ett webbmejlprogram sköter kontakten mellan mejlserver och webbserver och skapar de webbsidor som används för användargränssnittet.

SMTP-protokollet är konstruerat så att mejl inte ska kunna försvinna på grund av nätverksstörningar eller liknande. Den vanligaste orsaken till att mejl inte kommer fram på avsett vis är därför inte ett oförutsett avbrott på väg till mottagaren, utan att mejlet klassificeras som skräppost.

Att skicka e-post liknas ofta vid att skicka ett vykort utan kuvert med posten. Dock kan det argumenteras för att vykort förmodligen är ett säkrare val, eftersom dessa passerar betydligt färre potentiella läsare än ett genomsnittligt mejl. På väg till mottagaren passerar ett mejl via en mängd servrar anslutna till nätet. Vid varje enskild punkt är det i regel enkelt att läsa vad som står skrivet i mejlet. Texten i mejlet kan även läsas av den enskildes mejlleverantör och internetleverantör. Detta beror på att mejl vanligen skickas över nätet i klartext – som bokstäver, siffror och andra tecken – och därmed kan läsas var som helst längs vägen, och även lagras i klartext. I mejltekniken finns inga inbyggda säkerhetsåtgärder som döljer innehållet för andra än mottagaren. Den gör det heller inte möjligt att för avsändare få veta om någon, och i sådana fall vem, som har tagit del av informationen som skickats. En angripare som vill komma över kommunikationen kan därför med hjälp av ett program spela in all trafik som rör sig in och ut från en enskild persons dator.[18]

[18] Internetstiftelsen i Sverige, IIS, Internetguide nr 30, *IT-säkerhet för privatpersoner*, version 1.0, 2013, av Daniel Goldberg och Linus Larsson.

För att skydda innehållet i meddelanden från antingen förvanskning eller insyn används elektroniska signaturer respektive kryptering. Det existerar i huvudsak två standardiserade metoder för att skapa elektroniska signaturer eller kryptera innehållet i mejl, S/MIME och PGP.

En kryptografisk signatur säkerställer att meddelandet inte förvanskats från det att signaturen skapades till dess att mottagaren verifierar signaturen på meddelandet. Det görs genom att skapa en kryptografiskt säker checksumma av meddelandet och kryptera denna checksumma med avsändarens hemliga nyckel. Då mottagaren dekrypterar checksumman med avsändarens publika nyckel kan mottagaren dels verifiera att avsändaren också är innehavaren av den privata nyckeln, samt genom att verifiera checksumman också verifiera att meddelandet inte har förvanskats på vägen. Ett krypterat meddelande är krypterat med mottagarens (det kan vara flera) publika nyckel, och eftersom modernt krypto är asymmetriskt kan således också bara mottagarna dekryptera meddelandet. Oftast signerar man krypterade meddelanden för att bevisa att avsändaren är autentisk.

Genom kryptering kan alltså mejlets innehåll skyddas från att läsas av andra än den avsedda mottagaren. Däremot visas fortfarande både avsändarens och mottagarens adresser samt en hel del annan information som till exempel vid vilken tid och vilket datum mejlet skickades. För den som även är mån om att skydda sin och mottagarens identiteter, behövs därför fler åtgärder än kryptering, som exempelvis anonyma och temporära mejladresser.

För att säkert utbyta information mellan e-postservrar behöver kommunikationen skyddas under transport. TLS (akronym för engelskans Transport Layer Security, ungefär transportlagersäkerhet på svenska) är en öppen standard för säkert utbyte av krypterad information mellan datorsystem (dvs. till skillnad från kryptering som görs av den enskilde avsändaren och som berörs ovan). TLS används för att kryptera kommunikationen mellan två enheter. Tanken med att skydda den information som utväxlas mellan dessa enheter är att ingen annan på nätverket, till exempel internet, ska kunna avlyssna eller förvanska informationen. TLS erbjuder förutom konfidentialitet (kryptering) även riktighet (dataintegritet), och

beroende på hur det används dessutom äkthetsskydd (källskydd). TLS kan alltså användas vid överföring av mejl (SMTP), vilket är bra i de fall då man inte använder sig av kryptering på meddelandenivå.[19]

Dagens mejlprogram innehåller också en del funktioner som ökar riskerna för att mejlet skickas fel. Det kan vara namn och e-postadresser som fylls i automatiskt eller upprättade mejllistor som gör att mejlet oavsiktligt riskerar att skickas till fel mottagare eller till betydligt fler mottagare än avsändaren avsett. Det är också enkelt att förfalska en avsändaradress om inga åtgärder vidtagits för att förhindra detta. Inom IETF[20] har standarder utvecklats i syfte att förhindra sådana förfalskningar. DomainKeys Identified Mail (DKIM) är en teknik som genom digitala signaturer skyddar valda delar av e-posthuvudet och innehållet i e-postmeddelandet från modifiering av tredje part. Den viktigaste komponenten som skyddas är avsändaradressen. Detta för att motverka förfalskade avsändaradresser i syfte att förhindra nätfiske och andra typer av attacker.

Enligt Datainspektionen har den senaste tiden teknikutveckling inneburit att resonemang kring ”interna” mejl (dvs. tanken att mejl som skickas inom en organsation inte kan läsas av obehöriga utanför organisationen) allt mer har förlorat sin relevans. Anledningen till detta är bl.a. att om det finns funktioner för webbmejl, innebär dessa så gott som alltid att mejlen görs tillgänglig via ett öppet nät. Detsamma gäller om vissa tjänster, till exempel antivirusfunktioner eller spamtvätt, tillhandahålls av en extern leverantör. Om hela eller delar av drift, administration eller underhåll av mejlsystemet läggs ut på en extern part, ett personuppgiftsbiträde, tillkommer frågor om hur denne går till väga för att logga in till e-postsystemet. Funktioner för distansadministration används ofta över öppet nät.[21]

Trots de inbyggda säkerhetsbristerna i tekniken, används e-post mycket flitigt på många håll i samhället. E-post är i dag den mest använda tjänsten för att skicka meddelanden över nätet och är alltså fortfarande vanligare än att skicka meddelanden genom sociala nät-

[19] Rapporten *Elektronisk post med kvalitet och finess – vad och hur gör man?* publicerad av Internetstiftelsen i Sverige, IIS, författad av Anne-Marie Eklund Löwinder.

[20] Internet Engineering Task Force (www.ietf.org).

[21] Säkerhet för personuppgifter i e-post. Datainspektionen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sakerhet-enligt-personuppgiftslagen/sakerhet-for-personuppgifter-i-e-post/ Hämtat 2016-05-10.

verk. Under år 2015 användes e-post dagligen av 62 procent av alla internetanvändare i Sverige (siffran gäller personer äldre än 12 år, även om e-post också används av yngre barn). [22]

Mejlteknikens tillförlitlighet när det gäller att snabbt leverera meddelanden, medför att den också är en mycket vanlig kommunikationsform på många arbetsplatser, även myndigheter. Vi har inte funnit några undersökningar som visar hur vanligt det är att känsliga personuppgifter mejlas okrypterat på arbetsplatser och myndigheter. Det finns dock anledning att anta att detta inte är något ovanligt fenomen, mot bakgrund av hur vanlig och lättanvänd tekniken är. Tittar man dessutom på hur begränsad användningen av kryptering faktiskt är så stärks det antagandet ytterligare.

Datainspektionen har i flera tillsynsärenden konstaterat att personuppgiftsanvariga företag och myndigheter saknat tillräckligt tydliga policyer för sin hantering av personuppgifter i e-post.[23]

13.3 Det skyddande regelverket

Personuppgiftslagen

Personuppgiftslagens (1998:204) bestämmelser gäller för det sociala mediets hantering av personuppgifter. Av särskild betydelse är i detta sammanhang personuppgiftslagens bestämmelser om ändamålsbegränsning, samtycke, information och säkerhetsåtgärder.

När enskilda användare publicerar uppgifter om andra personer på ett socialt medium, är det i regel 5 a § i personuppgiftslagen som ska tillämpas. Enligt Datainspektionen innebär bestämmelsen att om personuppgifter publiceras i en löpande text på internet, till exempel i en blogg, är publiceringen i princip tillåten så länge man inte kränker den som personuppgifterna handlar om. Det är inte möjligt att generellt slå fast vad som är en kränkning av den personliga integriteten utan man måste göra en bedömning i varje enskilt fall och väga in samtliga omständigheter. Faktorer som påverkar bedömningen är bland annat syftet med publiceringen, vilka uppgifter som publiceras,

[22] *Svenskarna och internet, 2015 års undersökning av svenska folkets internetvanor*, utgiven av Internetstiftelsen i Sverige, IIS, författad av Olle Findahl och Pamela Davidsson.

[23] Se t.ex. Datainspektionens beslut den 24 februari 2012 med dnr 752-2011 samt beslut den 17 november 2014 med dnr 1713-2013. I dessa ärenden granskades ett universitets rutiner för hantering av känsliga personuppgifter i e-post.

var dessa publiceras, vilken information som har lämnats och hur länge uppgifterna publicerats på internet. Hur den vars uppgifter publiceras själv upplever publiceringen kan vara av betydelse, men är inte avgörande för om det ska anses vara fråga om kränkning i personuppgiftslagens mening. Att publicera personuppgifter i syfte att skandalisera eller ”hänga ut” någon är tydliga exempel på publicering som normalt är kränkande enligt personuppgiftslagen.[24]

När det gäller mejl, är det särskilt 31 § personuppgiftslagen som är aktuell. Enligt denna bestämmelse, såsom den tolkats i praxis, gäller generellt att känsliga personuppgifter som kommuniceras över öppna nät, som exempelvis internet, ska skyddas på ett sådant sätt att obehöriga inte kan ta del av uppgifterna. Det gäller även för mejl och innebär i praktiken att känsliga personuppgifter i mejl ska krypteringsskyddas på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem.

Brottsbalken

I februari 2016 lämnade Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten betänkandet *Integritet och straffskydd*.[25] I betänkandet föreslås bl.a. en ny straffbestämmelse om s.k. olaga integritetsintrång i 4 kap. brottsbalken. Den föreslagna bestämmelsen innebär ett straffansvar för den som gör intrång i någon annans privatliv genom att sprida bild eller annan uppgift på ett sätt som är ägnat att medföra kännbar skada för den som uppgiften rör.

Sociala medier utanför svensk jurisdiktion

Personuppgiftslagen gäller endast för sådana personuppgiftsansvariga som är etablerade i Sverige, samt för personuppgiftsansvariga i tredje land som använder sig av utrustning som finns i Sverige för att behandla personuppgifter.

[24] Datainspektionens broschyr *Publicering på Internet*, daterad februari 2012.
[25] SOU 2016:7.

Det betyder att sociala medier som inte är etablerade i Sverige, och som heller inte använder sig av exempelvis en server som finns i Sverige, inte behöver tillämpa personuppgiftslagen, även om det är uppgifter om personer som finns i Sverige som hanteras i det sociala mediet. Andra länders lagstiftning kan då komma att gälla. I exempelvis USA regleras hanteringen av personuppgifter i sociala medier av lagstiftning på federal nivå, endast om det är frågan om uppgifter om barn under 13 års ålder. Då gäller den s.k. COPPA (Children's Online Privacy Protection Act). Lagen innehåller bl.a. bestämmelser om information till vårdnadshavare och inhämtande av samtycke från vårdnadshavarna. För uppgifter om vuxna eller äldre barn saknas det på federal nivå en motsvarighet till EU:s relativt heltäckande dataskyddsdirektiv, både för sociala medier och för uppgifter om konsumenter överhuvudtaget.

Överföring till USA

Många sociala medier hanterar uppgifter i USA, även om sina europeiska kunder. Ett utlämnande av uppgifter till s.k. tredje land (land utanför EES-området) regleras i personuppgiftslagens 33–35 §§. Huvudregeln är att tredjelandsöverföring är förbjuden till länder som inte har en adekvat nivå för skyddet av personuppgifter.

Överföring var tidigare dock tillåten till bolag i USA som är anslutna till Safe Harbor-principerna, eftersom EU-kommissionen beslutat att skyddsnivån i sådana fall skulle anses som adekvat. Systemet med Safe Harbor-principerna inbegriper ett antal principer angående skydd för personuppgifter vilka amerikanska företag frivilligt kan ansluta sig till, enligt EU-kommissionens beslut.[26]

EU-domstolen har dock nyligen ogiltigförklarat kommissionens beslut.[27] I målet var frågan om en österrikisk medborgare som invänt mot att Facebook överför uppgifter om honom till USA. Som skäl för avgörandet anför EU-domstolen bl.a. följande. Systemet med Safe Harbor-principerna är endast tillämpligt för de amerikanska

[26] Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, s. 7).

[27] EU-domstolens dom den 6 oktober 2015 i mål C-362/14, *Maximillian Schrems mot Data Protection Commissioner*.

företag som anslutit sig till det. Förenta staternas myndigheter är inte själva bundna av det. Vidare har krav i fråga om den nationella säkerheten i Förenta staterna företräde framför Safe Harbor-systemet. Detta innebär att amerikanska företag är skyldiga att utan inskränkningar frångå systemets skyddsregler när de står i konflikt med sådana krav. Det amerikanska Safe Harbor-systemet möjliggör således ingrepp från de amerikanska myndigheternas sida i enskilda personers grundläggande rättigheter. I kommissionens beslut anges att det i Förenta staterna varken finns regler som syftar till att begränsa sådana eventuella ingrepp, eller något effektivt rättsligt skydd mot dessa.

Vidare påpekar EU-domstolen att en lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, kränker det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, eftersom en sådan möjlighet är en grundförutsättning för en rättsstat.

EU-domstolens dom innebär att en överföring av personuppgifter från ett EU-land till USA inte längre kan göras enbart med stöd av att det mottagande företaget i USA är anslutet till Safe Harbor-principerna.

Som en följd av detta, enades i februari 2016 EU-kommissionen och USA på ett övergripande plan om en ny ordning för transatlantiska dataflöden, kallad för ”sköld för skydd av privatlivet” (på engelska privacy shield). Artikel 29-gruppen har granskat dokumenten som ligger till grund för överenskommelsen och välkomnar de förbättringar som den innehåller jämfört med Safe Harbour-principerna. Artikel 29-gruppen hyser dock stora betänkligheter på en rad punkter beträffande både de kommersiella aspekterna och beträffande myndigheternas åtkomst, när uppgifter överförs med stöd av den nya överenskommelsen. Artikel 29-gruppen uppmanar därför Kommissionen att lösa de utestående problemen med överenskommelsen och förbättra den så att den ger ett skydd som motsvarar EU:s dataskyddsregler.[28]

[28] *Statement of the Article 29 Working Party on the opinion on the EU-U.S. Privacy Shield*, den 13 April 2016.

Lagen om avtalsvillkor i konsumentförhållanden

Även lagen (1994:1512) om avtalsvillkor i konsumentförhållanden kan bli tillämplig på hanteringen av personuppgifter i sociala medier. Enligt lagen kan oskäliga avtalsvillkor förbjudas. Exempel på oskäliga avtalsvillkor är villkor som leder till en så stor nackdel för konsumenten att det inte blir en rimlig balans mellan näringsidkarens och konsumentens rättigheter, till exempel när endast näringsidkaren kan säga upp avtalet. Som oskäliga anses också villkor som är vilseledande eller oklart formulerade och innebär att konsumenten blir vilseledd om sina rättigheter, till exempel villkor som är motsägelsefulla eller ofullständiga.

I Frankrike har konsumentskyddsmyndigheten Commission des clauses abusives år 2014 formulerat rekommendationer för hur sociala medier bör utforma sina avtalsvillkor. Flera av rekommendationerna rör avtalsvillkor om hanteringen av personuppgifter. Myndigheten pekar inledningsvis på problemet att sociala medier vill få konsumenten att tro att deras tjänster är helt och hållet gratis och att det inte förväntas någon motprestation av konsumenten som använder sig av mediet, medan motprestationen i själva verket består av de personuppgifter som användarna lämnar till det sociala mediet. Därefter rekommenderar myndigheten bland annat att avtalsvillkor inte ska innehålla formuleringar som får konsumenten att tro att hennes eller hans personuppgifter får lämnas ut till ospecificerade tredje parter, utan att samtycke inhämtas i förväg eller att konsumenten åtminstone i efterhand kan komma med invändningar mot utlämnandet.

Det finns inga motsvarande rekommendationer om sociala mediers avtalsvillkor om personuppgifter från det svenska Konsumentverket.

13.4 Kommitténs samlade bedömning av området

En stor del av landets befolkning, särskilt yngre och kvinnor, använder dagligen sociala medier för att lagra och publicera en mycket stor mängd uppgifter och för att utbyta privat information med andra användare.

Sociala medier kan föra med sig många fördelar för de enskilda användarna, i form av exempelvis nya möjligheter till både kunskap och utbyte med andra. Ur ett integritetsskyddsperspektiv finns det emellertid även en rad risker med användningen av sociala medier.

Användarvillkor är ofta långa och krångligt skrivna. Även i de få fall då användaren faktiskt tagit del av villkoren, är dessa inte sällan så otydliga att många användare inte ens förstår vilka andra användare som kan ta del av uppgifterna han eller hon har publicerat på det sociala mediet, och än mindre för vilka egna ändamål som det sociala mediet kan använda sig av uppgifterna. Användarvillkoren är också ofta vaga när det gäller till vilka samarbetsparter det sociala mediet får sprida uppgifterna och hur dessa får vidareanvändas. Användarvillkoren kan också innehålla oklarheter beträffande hur länge uppgifterna lagras i någon form hos det sociala mediet. Mot den bakgrunden kan det ofta vara mycket svårt för en enskild användare att bilda sig en egen uppfattning om vilka konsekvenser för den personliga integriteten som användningen av det sociala mediet faktiskt innebär.

Särskilt allvarlig är den risken när det gäller unga, som i dag kan vilja lagra och publicera texter och bilder som de senare i livet skulle vilja radera från nätet, men som kanske inte kommer att ha den möjligheten, på grund av villkor som en gång accepterats, eller på grund av att uppgifterna har spridits till tredje parter hos vilka varken användaren eller det sociala mediet har något som helst inflytande över hur uppgifterna används.

Ett specialfall av detta är situationen då uppgifter om mycket unga personer lagras eller publiceras av deras föräldrar. När barnen efter hand blir medvetna om hanteringen av uppgifter om dem, kommer det i de flesta fall vara omöjligt för dem att hindra eller ens överblicka spridningen och användningen av uppgifterna.

Förutom att hanteringen är svår att överblicka utifrån användarvillkoren, ger villkoren ofta mycket fria händer åt det sociala mediet att använda sig av uppgifterna för egna ändamål. Särskilt när möjlighet finns att tillföra andra stora mängder uppgifter till uppgifterna från det sociala mediet och sambearbeta dessa, blir det i praktiken omöjligt för användaren att i förväg veta för vilka ändamål uppgifterna kan komma att användas.

I och med att ny teknik utvecklas kommer alla uppgifter som lagras och publiceras i sociala medier att kunna användas för en allt mer detaljerad och närgången kartläggning bortom användarnas kännedom eller kontroll.

Eftersom sociala medier oftast är baserade på molntjänster som hanterar uppgifterna utanför EES, finns det också en stor risk för att uppgifter om användarna hamnar i länder där lagstiftningen ger ett otillräckligt skydd. Det kan leda till att exempelvis underrättelsetjänster eller andra myndigheter och organisationer utanför EES lagligen kan få åtkomst till uppgifterna för ändamål och på ett sätt som inte hade varit lagligt i Sverige eller i något annat land inom EES.

Användningen av vissa sociala medier kan medföra att ett stort antal närgångna uppgifter om den enskilde oavsiktligen exponeras för andra användare. Vidare förekommer det att sociala medier använder uppgifterna för egna ändamål och sprider dem vidare till andra företag. Vanligtvis är det också svårt för användarna att få klarhet i vilken hantering som kan förekomma, när användarvillkoren väl har godkänts. Den enskildes valmöjlighet är ofta begränsad till att antingen godkänna samtliga villkor, eller att avböja och därmed helt ställa sig utanför det sociala mediet. Sammantaget anser kommittén att användningen av sociala medier som har de nyss nämnda egenskaperna innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att även sådana sociala medier kan medföra en mycket stor nytta för den enskilde och för samhället i stort, och att många tjänster är mycket populära bland användarna.

En annan risk för den enskildes personliga integritet ligger i vad användare av sociala medier kan skriva och publicera om andra personer. Genom internet och annan elektronisk kommunikation har möjligheterna för enskilda att sprida integritetskränkande uppgifter om andra ökat väsentligt. Nya skyddsintressen har därför uppkommit och medfört ett väsentligt ökat behov av ett bättre utformat straffrättsligt skydd för privatlivet och den personliga integriteten. Med den motiveringen föreslås i betänkandet *Integritet och straffskydd*[29] en ny straffbestämmelse om s.k. olaga integritetsintrång som tar sikte på kränkningar som enskilda personer begår mot andra enskilda.

[29] SOU 2016:7.

Om oskyddad e-post används för att skicka integritetskänsliga uppgifter, innebär det att uppgifterna kan användas för egna ändamål av de företag som vidarebefordrar meddelandet, även om det görs i strid mot lag. Vidare kan antagonistiska aktörer få åtkomst till uppgifterna genom t.ex. avlyssning. Många organisationer har policyer som ska begränsa möjligheterna att i mejl skicka integritetskänsliga uppgifter om enskilda, men dessa policyer är inte sällan otydliga och dessutom är det svårt att kontrollera hur de följs. Sammantaget bedömer kommittén därför att användning av e-post innebär en påtaglig risk för den personliga integriteten.

14 Försäkringsverksamhet

Kommitténs bedömning: Det finns påtagliga risker för den personliga integriteten i samband med försäkringsföretagens verksamhet.

Den framtida hanteringen av personuppgifter inom försäkringsverksamheten kan innefatta allvarliga risker för den personliga integriteten.

14.1 Om försäkring och hantering av personuppgifter

14.1.1 Vad är försäkring?

Försäkring är ett sätt för en individ att hantera en osäkerhet. I utbyte mot en liten, men känd, kostnad skyddar en försäkring mot en stor ekonomisk förlust som kan uppstå, någon gång i framtiden. En av de grundläggande tankarna med en försäkring är att den ska verka riskutjämnande mellan en grupp personer. Eftersom alla försäkrade inte exponeras för samma risker varierar premien bland de försäkrade. Premien på en livförsäkring påverkas exempelvis av ålder, en fordonsförsäkring av årlig körsträcka och bostadsort. Däremot är det inte längre tillåtet att låta försäkringstagarens kön påverka storleken på premien.

I betänkandet *Lönegarantiförsäkring – en partsfråga*[1], förklaras försäkring så här:

> Försäkring innebär tekniskt sett en utjämning över tiden och över kollektivet av slumpmässigt uppträdande av förluster bland dem som ingår i ett kollektiv. I försäkring tillämpas de stora talens lag; ju större och mer likartad

[1] Utredningens om finansieringen av lönegarantin betänkande *Lönegarantiförsäkring – en partsfråga*, SOU 2004:93.

en grupp är desto säkrare kan man beräkna framtida ersättningar och vilken premie som krävs. Gruppen behöver i regel också bygga upp reserver för slumpmässiga variationer i skadefrekvens och skadestorlek.

”De stora talens lag” är en del av sannolikhetsläran och ett i sammanhanget viktigt begrepp. För försäkringsföretag är det givetvis av största betydelse att ha bra matematiska modeller för vilka försäkringsfall som kommer att uppstå. Och ju bättre underlaget för modellerna är, desto träffsäkrare blir prognoserna.

14.1.2 Behov av behandling av personuppgifter inom försäkringsföretagen

Försäkringsföretagen behöver behandla personuppgifter för premieberäkning, statistik, marknadsföring, skadereglering och för förebyggande av skador. Vidare används personuppgifterna för att uppfylla skyldigheter enligt lag och andra författningar, till exempel försäkringsrörelselagen (2010:2043), finansinspektionens författningar och skattelagstiftningen. Personuppgifterna används också för exempelvis utredning av oklara försäkringsfall.

14.1.3 Den rättsliga regleringen

Behandlingen av personuppgifter hos försäkringsföretag regleras i första hand i personuppgiftslagen (1998:204). Regleringen i personuppgiftslagen behandlas närmare i kapitel 6, *Det grundläggande rättsliga skyddet.*

Den allmänna regleringen i personuppgiftslagen kompletteras av vissa bestämmelser som tar sikte på försäkringsföretagens verksamhet, t.ex. i försäkringsrörelselagen och försäkringsavtalslagen (2005:104). Där finns bestämmelser som t.ex. reglerar den upplysningsplikt som försäkringstagaren har mot försäkringsföretaget avseende uppgifter som har betydelse för avtalet och om under vilka förutsättningar företaget får hämta in samtycke från försäkringstagaren till att hämta in uppgifter om den enskildes hälsotillstånd.

Det finns inga generella sekretessbestämmelser som gäller för hantering av personuppgifter hos försäkringsföretag. Däremot tillämpas inom försäkringsbranschen en frivilligt påtagen tystnads-

plikt.[2] När det gäller uppgifter om genetisk undersökning eller genetisk information finns det dock en lagstadgad tystnadsplikt i försäkringsrörelselagen. Därtill finns en viss lagreglerad begränsning när det gäller att lämna ut uppgifter från försäkringsföretag genom bestämmelserna om på vilket sätt personuppgifter får behandlas enligt personuppgiftslagen. Uppgifter får endast lämnas ut om det inte är oförenligt med det ändamål för vilket uppgifterna har samlats in.

Företag som bedriver livförsäkringsrörelse omfattas även av lagen om (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism.

14.1.4 Tillsyn m.m.

Datainspektionen utövar tillsyn över försäkringsföretagens behandling av personuppgifter enligt personuppgiftslagen.

Finansinspektionen ansvarar för att ge tillstånd att bedriva försäkringsrörelse och för tillsynen av försäkringsföretagen.

14.1.5 Branschöverenskommelser

Svensk Försäkring[3] är försäkringsföretagens branschorganisation. Organisationen utfärdar bl.a. gemensamma branschrekommendationer som gäller alla medlemsföretag. Det finns t.ex. rekommendationer om behandling av personuppgifter inom försäkringsföretagens utredningsverksamhet, om behandling av personuppgifter om hälsa inom försäkringsbranschen, om förköpsinformation och om hantering av genetisk information.

[2] Svensk Försäkrings Rekommendation om behandling av personuppgifter om hälsa inom försäkringsbranschen.

[3] www.svenskforsakring.se

14.2 Behandling av uppgifter för att bedöma premier m.m.

14.2.1 Försäkring och modern teknik

Med ny teknik kommer möjligheten att basera premien på nya faktorer. För en personförsäkring kan t.ex. den försäkrades vardagsmotion, som den registreras av en aktivitetsmätare, vara en faktor. Aktivitetsmätare är en relativt ny typ av konsumentprodukt som med rörelsesensorer känner av hur användaren rör sig och med hjälp av olika algoritmer (mer eller mindre säkert) kan avgöra exempelvis hur många steg han eller hon har gått under dagen. Fitbit och Jawbone är två av de mest kända företagen som säljer aktivitetsmätare. Men även smarta klockor, som Apple Watch, har sådana funktioner. För en fordonsförsäkring kan t.ex. vägval, registrerat av en GPS, användas.

Ett av de vanligaste argumenten för att använda modern teknik i försäkringssammanhang är att det kan åstadkomma en rättvisare riskfördelning i form av mer differentierade försäkringspremier.[4] En person som rör sig mycket minskar risken för många sjukdomar och bör enligt detta resonemang betala en lägre premie för sin sjukförsäkring än den som lever ett mer stillasittande liv. Och en person som i stor utsträckning kör sin bil på motorväg med få olyckor kan få betala en lägre premie för sin fordonsförsäkring än den som i stället ofta färdas på en olycksdrabbad landsväg.

Men denna utveckling har också flera integritetsaspekter. Det handlar om hur den insamlade informationen används och hur den skyddas mot obehörig spridning. Både hälsodata som samlas in av aktivitetsmätare och positionsuppgifter om var en försäkrad bil befinner sig är känslig information. Alla de risker som behandlas i avsnitt 21.1 om molntjänster gäller i högsta grad de tillämpningar som tas upp i denna text. Lagras informationen på ett sätt som skyddar den mot externa attacker? Hur säkerställs att bara behörig personal kommer åt den? Gallras uppgifterna när de inte längre behövs?

[4] The Economist, *Risk and reward – Data and technology are starting to up-end the insurance business*, publicerad den 14 mars 2015 på www.economist.com

14.2.2 Ny teknik ger nya bedömningsgrunder

Med teknikutvecklingen har försäkringsföretagen fått nya möjligheter att bland annat värdera risk. Det handlar t.ex. om teknik som företagen själva utrustar sina kunder med, i form av aktivitetsmätare som registrerar människors rörelser och motsvarande lösningar för fordon. Men det handlar också om analys av data från andra datakällor. På motsvarande sätt som i banksektorn[5] och många andra branscher har det framkommit att åtminstone utländska försäkringsföretag använder *big data*-verktyg för att dra slutsatser ur exempelvis information som samlas in från sociala medier.

För personförsäkringar ligger i dag faktorer som ålder och svar på hälsodeklarationer till grund för premiens storlek och för om personen i fråga alls ska godkännas som försäkringstagare. När det gäller fordonsförsäkringar används bland annat ägarens ålder, årlig körsträcka och bostadsadress. Alla dessa exempel är faktorer som försäkringsföretagens analyser har visat påverkar risken för att ett försäkringsfall ska uppstå, och som därmed också ligger till grund för kostnaden för försäkringstagaren. Just person- och fordonsförsäkringar är två produktkategorier där försäkringsföretagen sedan några år tillbaka börjat utforska teknikens möjligheter. Med teknikens hjälp har det ju blivit möjligt att mäta både en människas och en bils ”aktiviteter”. Förutom produkter som mäter rörelse finns det också sådana som sägs kunna mäta användarens stressnivå och andra som mäter blodsockernivåer. För personer som medicinerar mot en sjukdom handlar personlig hälsa också om att rätt läkemedel tas vid rätt tidpunkt. Det utvecklas t.ex. läkemedelsförpackningar som kan påminna användaren om det.

Företag som amerikanska 23andme[6] erbjuder konsumenttjänster för DNA-analys, där kunderna får reda på om deras arvsmassa påverkar risken för att drabbas av ett antal sjukdomar.

Företag som säljer fordonsförsäkringar använder ofta en modell som går under namnet *usage-based insurance, UBI*. Det innebär att premien beräknas utifrån hur fordonet faktiskt används. I sin allra enklaste form sätts premien utifrån en årlig körsträcka, där utgångspunkten är att risken ökar med antalet körda mil.

[5] Se kapitel 15 om bank och kreditmarknaden.
[6] 23andme – https://www.23andme.com

Men också för fordon finns produkter som påminner om aktivitetsarmbanden. På motsvarande sätt som vid användning av aktivitetsarmband kan fordon förses med rörelsesensorer som bland annat används för att registrera hur föraren accelererar, bromsar och svänger, medan en GPS loggar på vilka vägar bilen förs fram. Ofta ansluts utrustningen till en kontakt i bilen som kallas *OnBoard Diagnostic*. Den insamlade information används sedan av försäkringsföretagen för att bedöma risknivån. Återkommande häftiga inbromsningar kan exempelvis tyda på bristande uppmärksamhet, medan resor utanför rusningstrafik och på vägar med få olyckor är en positiv signal.

De nya möjligheter som försäkringsföretagen tack vare teknikutvecklingen får till sitt förfogande är i många fall en vidareutveckling av de analyser och bedömningar som redan görs. Exempelvis kan försäkringstagare som inte anmält försäkringsärenden gällande sitt fordon få rabatt på premien. Men att ett fordon inte har varit inblandat i en olycka säger inte med nödvändighet något om hur bilen framförts, vilket däremot en analys av de uppgifter som samlas in av den nya utrustningen kan göra. Förespråkarna för *usage-based insurance* för fordon brukar lyfta fram ett antal potentiella fördelar, exempelvis:[7]

– Rättvisare premier när försäkringsföretagen genom tekniken får möjligheter att göra bättre segmentering av sina kunder. Det kan till exempel innebära att unga men försiktiga och/eller duktiga förare som i dag får betala höga premier på grund av sin låga ålder kan sänka sina försäkringskostnader.
– En säkrare trafikmiljö, förutsatt att lägre premier som konsekvens av försiktigare körstil har tillräckligt stor attraktionskraft.
– Minskade utsläpp, med samma reservation som för en säkrare trafikmiljö.

[7] Usage-based insurance, Wikipedia – https://en.wikipedia.org/wiki/Usage-based_insurance

14.2.3 Insamling av kördata

Hösten 2015 började två svenska försäkringsföretag med en försäkring där premien beräknas på försäkringstagarens beteenden. Det handlar om fordonsförsäkring vars premier ska beräknas på förarens körsstil. Det görs genom en app som installeras i försäkringstagarens mobiltelefon. Telefonens inbyggda sensorer används tillsammans med GPS:en för att avgöra hur personen är som bilförare: hastighet, inbromsningar, acceleration, kurvtagning och total körsträcka samlas in. Informationen kombineras med data om hastighetsbegränsningar som hämtas från Transportstyrelsens vägdatabas. I en av lösningarna används en indikator i bilen tillsammans med appen. Indikatorn visar för föraren om hastighetsbegränsningarna hålls under färd. Varje tur med bilen kan sedan analyseras av försäkringsföretaget. Information om de samlade resorna vägs samman till en eventuell premierabatt på 15–20 procent.

Företagen presenterar på sina respektive webbplatser hur det är tänkt att uppgifter som samlas in genom denna lösning ska användas. Båda företagen uppger att de bara kommer att använda information om varje körning i aggregerad form för att kunna beräkna premien. Inga uppgifter som kopplar samman tid och plats för körning med person kommer enligt bolagen att sparas. Båda företagen avser att använda anonymiserade uppgifter för produktutveckling.

14.2.4 Aktivitetsmätare

Under våren 2016 har ett svenskt försäkringsföretag lanserat en sjuk- och olycksfallsförsäkring som ger rabatt på premien när kunden rör på sig i vardagen. Försäkringen är kopplad till en mobilapp som mäter hur många steg kunden tar varje dag. Ju mer försäkringstagaren rör på sig i vardagen desto högre rabatt. Den som går minst 7 500 steg per dag får 5 procents rabatt. För att få den maximala rabatten på 15 procent ska försäkringstagaren gå 9 500 steg per dag utslaget på en 30-dagars period.

Det finns sedan tidigare utländska försäkringsföretag som använder aktivitetsmätare för att beräkna premier på personförsäkringar. Amerikanska Oscar[8] är ett försäkringsbolag som säljer personför-

[8] Oscar's Experience – https://www.hioscar.com/experience/

säkringar. Kunder kan få en gratis aktivitetsmätare, en Misfit. När kunden sitt aktivitetsmål ger det upp till en dollar per dag i bonus. Amerikanska John Hancock är ett andra exempel på försäkringsbolag som jobbar med aktivitetsmätare. Tillsammans med brittiska Vitality erbjuder JohnHancock sina kunder ett bonussystem liknande Oscars.[9]

14.2.5 Data från andra källor

I takt med att allt fler delar av samhället digitaliseras i allt större utsträckning uppstår allt fler informationskällor som går att använda för olika typer av analyser. Precis som i andra branscher kan och kommer försäkringsföretag att använda data som samlas in från exempelvis sociala medier. Många förutspår också en snar tillväxt för olika typer av uppkopplade prylar, det som kallas för *internet of things eller sakernas internet*, vilket kommer få tillgången till data att växa ytterligare. Med tillräckligt stora datamängder i kombination med avancerade analysverktyg blir detta ett viktigt verktyg för många företag, i försäkringsbranschen och på annat håll.

I en artikel i The Economist våren 2015 anfördes bl.a. att modern teknik gör det möjligt för försäkringsbolagen att mäta individuella risker mycket mer exakt. Digitala spår i sociala medier, uppgifter om kreditkortsanvändning och andra registrerade uppgifter ger upphov till mängder av information. I ett pilotprojekt av en brittisk försäkringsgivare verksam i USA iakttogs att analyser av en potentiell kunds mindre konventionella data, till exempel online-beteende och köpvanor, var ett lika effektivt sätt att identifiera potentiella hälsorisker som att analysera medicinska hälsoundersökningar.[10] I artikeln lyftes även fram hur Facebook-flöden och information om vad en person gillar kan användas för att göra antaganden om försäkringsrisker.

Bakom försäkringsbranschens ökande teknikanvändning finns flera drivande faktorer. Den mest uppenbara handlar om att försäkringsföretagen vill bli bättre på att förutse och hantera risker. Med ett växande beslutsunderlag i form av data, som samlas in från senso-

[9] John Hancock – http://www.jhrewardslife.com/

[10] *Risk and reward – Data and technology are starting to up-end the insurance business*, The Economist publicerad den 14 mars 2015 på www.economist.com

rer i olika former, kombinerat med de analysmöjligheter som *big data* innebär, får försäkringsföretagen just detta. Men det handlar också om nya möjligheter att kommunicera med kunderna.

Hos försäkringsföretagen finns förhoppningar om att tekniken ska minska de totala kostnaderna. Om kostnaderna för en aktivitetsmätare och den bonus som försäkringstagaren får när denne använder mätaren understiger de beräknade kostnaderna för framtida försäkringshändelser som därmed kan undvikas är det en bra investering för försäkringsföretaget. I vilken utsträckning det verkligen blir utfallet är fortfarande osäkert. I en artikel om Oscars samarbete med Misfit konstaterar en av de intervjuade, Kevin Volpp, som är ansvarig för *Center for Health Incentives and Behavioral Economics* vid University of Pennsylvania, att det sannolikt är svårt att med en aktivitetsmätare sporra dem som mest behöver förändra sin livsstil.[11] Han anser att det sannolikt är lättare att få en person som redan går 8 000 steg om dagen att lockas av erbjudande om rabatt på premien om man uppnår 10 000 steg per dag, än en person som bara går 2 000 steg per dag.

I USA har arbetsgivare som tecknar gruppförsäkringar åt sina anställda också infört aktivitetsmätare i olika typer av hälsofrämjande bonusprogram. Syftet är att få fler i personalen att röra sig mer, och därmed kunna förhandla ner premierna gentemot försäkringsföretaget. Den här utvecklingen har inte gått företagen som tillverkar aktivitetsmätarna förbi.[12] Dagens Nyheter uppmärksammade i november 2015 detta att arbetsgivare vill kontrollera och påverka de anställdas hälsa.[13] I artikeln varnar lektorn i företagsekonomi Carl Cederström för denna utveckling och anför att gränserna mellan arbetet och fritiden suddas ut. Han menar att de anställda måste bete sig som arbetsgivarna vill i varje del av livet och att de på så sätt blir övervakade.

[11] Issie Lapowsky, *This Insurance Company Pays People to Stay Fit*, publicerad den 8 december 2014 på www.wired.com

[12] Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities – https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx

[13] Caroline Englund, *Nu vill arbetsgivarna hålla koll på din hälsa och träning*, publicerad den 26 november 2015 på www.dn.se

En annan relativt ny tänkbar källa för datainsamling är de olika former av egna ytor för hantering av personuppgifter som finns och som är under uppbyggnad, t.ex. olika former av hälsokonton där enskilda kan samla sina hälsouppgifter.

14.3 Exempel på risker för intrång i den personliga integriteten

14.3.1 Dataläckage

Mycket av den information som försäkringsföretagen är intresserade av att samla in är känslig. Exempelvis kan en dosa med GPS som kontinuerligt registrerar var en bil befinner sig avslöja mycket om ägarens vanor. Det samma gäller en aktivitetsmätare som registrerar fysisk aktivitet och sömn. Eftersom uppgifter som samlas in skickas vidare från användaren till molntjänstservrar innebär det att resonemangen i avsnittet (21.1) om *molntjänster* i allra högsta grad gäller detta specifika område. Det handlar t.ex. om säkerhetsarrangemang vid överförandet av uppgifter mellan exempelvis armband och server. Det handlar också om säkerhetsarrangemang när uppgifterna väl hamnat på servrarna. Hur ser skyddet mot externa attacker ut? Hur säkerställs att bara behörig personal kommer åt uppgifterna?

I februari 2015 drabbades Anthem, ett av de största personförsäkringsbolagen i USA, av ett stort dataintrång där 80 miljoner personuppgifter stals. I medierapporteringen förekom uppgifter om vad hälsodata är värt på den svarta marknaden. I en intervju med New York Times hävdade en säkerhetsexpert att priset på sådana uppgifter är upp till tio gånger högre än priset på ett stulet kreditkortsnummer.[14]

I avsnittet (21.2) om *big data* tas svårigheterna med att anonymisera insamlad data upp. Det finns forskning som visar att det är svårt att förhindra att information kan återkopplas till en viss individ, trots försök att anonymisera. Ett sätt att minska riskerna för den här typen av dataläckage är att helt enkelt låta bli att samla in informationen centralt. I stället för att t.ex. all rådata förmedlas från en försäkrings-

[14] Reed Abelson och Matthew Goldstein, *Anthem Hacking Points to Security Vulnerability of Health Care Industry*, publicerad den 5 februari 2015 på www.nytimes.com

tagares bil till försäkringsföretagets servrar kan beräkningarna göras i bilen. Då behöver bara ett faktureringsunderlag skickas vidare till företaget.

14.3.2 Dataanvändning

Hur försäkringsföretaget får använda den insamlade informationen är också en integritetsfråga. De försäkringsupplägg som hittills lanserats handlar till stor del om att försäkringstagaren med teknikens hjälp får möjlighet att visa för försäkringsföretaget att överenskomna villkor följs (”jag går 10 000 steg varje dag”) alternativt som underlag för framtida premieberäkningar (”jag gör ytterst få häftiga inbromsningar”). Men i dataunderlaget öppnar sig också nya möjligheter. Med verktyg för *big data*-analys finns exempelvis stora möjligheter att försöka hitta samband som kan användas för beräkning av risker.

I vilken utsträckning ska försäkringsföretag kunna använda hälsoinformation tillsammans med andra tillgängliga uppgifter? Sådan information kan användas för att dra slutsatser om exempelvis vilka andra produkter som sannolikt kan locka en viss kund eller om var dennes ekonomiska smärtgräns för försäkringskostnader går. Scott Peppet, professor vid University of Colorado School of Law som under en tid intresserat sig för hälsodata, varnar i en intervju för möjligheterna till utökad användning.[15] Han är bekymrad över uppgifterna om de anställdas aktivitet skulle kunna används för andra ändamål. t.ex. för att mäta de anställdas produktivitet eller för att delas med någon tredje part m.m.

14.3.3 Risk för diskriminering på försäkringsmarknaden?

En annan återkommande oro rör de effekter som aktivitetsmätare och liknande teknik kan få på försäkringsmarknaden och för möjligheterna för en individ att teckna en försäkring på lika villkor som andra. De som har råd att betala en hög fordonsförsäkring kan t.ex. fortsätta att köra vårdslöst. En ensamstående förälder kan däremot ha svårt att hinna med att både äta hälsosamt och träna och får då en

[15] Hamza Shaban, *Big Doctor Is Watching – How your fitness tracker could increase your health insurance costs someday*, publicerad den 27 februari 2015 på www.slate.com

högre premie för sin personförsäkring. Och en låginkomsttagare som lever väldigt hälsosamt, men som kanske inte har råd med de prylar som kan övertyga försäkringsföretagen om att så är fallet, får inte den belöning i form av en lägre premie som han eller hon egentligen skulle ha rätt till.

14.3.4 Inhämtning av uppgifter om hälsa

För att kunna bevilja en personförsäkring och reglera ett försäkringsfall krävs att försäkringsbolagen i vissa fall får tillgång till känsliga uppgifter om enskilda personers hälsotillstånd. Eftersom hälsouppgifter normalt är sekretessbelagda, måste den enskilde lämna sitt samtycke till att uppgifterna lämnas ut för att försäkringsbolaget ska få tillgång till uppgifterna. Med stöd av samtycket, som ofta benämns fullmakt, kan bolaget begära in t.ex. patientjournaler från hälso- och sjukvården.

I försäkringsavtalslagen finns regler om upplysningsplikt för försäkringstagare (dvs. den person för vars liv eller hälsa försäkringen gäller). Han eller hon är enligt 12 kap. 1 § skyldig att på försäkringsbolagets begäran lämna upplysningar som kan ha betydelse för frågan om en personförsäkring ska meddelas, utvidgas eller förnyas. Försäkringstagaren ska ge riktiga och fullständiga svar på försäkringsbolagets frågor. Bakgrunden är att det normalt endast är försäkringstagaren eller den försäkrade som har kunskap om de förhållanden som påverkar riskens storlek i det enskilda fallet.

På grund av att det har förekommit kritik mot försäkringsföretagens hantering av samtycken för att hämta in hälsouppgifter, infördes år 2011 nya bestämmelser i försäkringsavtalslagen som reglerade under vilka förutsättningar sådana samtycken får hämtas in. Enligt förarbetena[16] handlade kritiken för det första om utformningen och omfattningen av samtyckena till inhämtande av hälsouppgifter. Samtyckena ansågs vara otydliga, och att det därför fanns en risk för att den som lämnar ett samtycke inte insåg konsekvenserna av det. I det sammanhanget hade det även gjorts gällande att försäkringsbolagen fick tillgång till irrelevant information (överskottsinformation). För det andra hade det hävdats att det förekom att försäkringsbola-

[16] Regeringens proposition *Ett förstärkt integritetsskydd i försäkringssammanhang*, prop. 2009/10:241.

gen över- eller misstolkade informationen i journalerna med följd att försäkringstagare obefogat fick sämre villkor eller helt nekades försäkring. För det tredje hade vissa kritiker ansett att detta medförde risker för patientsäkerheten. Genom att vårdpersonalen anpassar sin journalföring till att försäkringsbolag kan komma att få del av journalen fanns det enligt kritikerna en risk för att viktiga uppgifter inte journalfördes. Denna kritik har särskilt gällt de journaler som förs inom barn- och skolhälsovården. Slutligen, och för det fjärde, hade det gjorts gällande att försäkringsbolag sparade den inhämtade informationen för länge och att informationen inte var skyddad eftersom det inte finns någon författningsreglerad tystnadsplikt för anställda i försäkringsbolag.

Regeringen ansåg att inhämtandet av hälsouppgifter som förutsätter den enskildes samtycke inte utesluter att det ändå brister i skyddet av den personliga integriteten. Ett samtycke kan lämnas t.ex. utan tillräcklig insikt i vad samtycket innebär eller till följd av att den enskilde upplever sig sakna reell möjlighet att vägra lämna samtycke på grund av att försäkringsskydd annars inte kan uppnås. En central utgångspunkt för regeringen var därför att de samtycken som förekommer i försäkringssammanhang ska vara frivilliga och bygga på tillräcklig information. Från och med 1 juli 2011 finns det därför bestämmelser i försäkringsavtalslagen som reglerar när försäkringsföretagen får begära samtycke till att inhämta hälsouppgifter.

Ändringarna i lagen innebär bl.a. att försäkringsbolaget vid en ansökan om individuell personförsäkring ska få begära samtycke till att inhämta hälsouppgifter endast om det är nödvändigt för prövningen av ansökan. Samtycke ska alltså få begäras först efter en individuell bedömning i varje enskilt fall. Försäkringsbolagets påstående att samtycket är nödvändigt ska – vid avslag på en försäkringsansökan – kunna prövas i domstol. Motsvarande ska gälla i samband med förnyelse av försäkring. Vid skadereglering ska försäkringsbolaget få begära samtycke till att inhämta hälsouppgifter först när det har uppkommit ett behov i det enskilda fallet. Samtycke ska alltså inte få begäras innan ett försäkringsfall har inträffat eller redan i skadeanmälan.

De nya reglerna om hur känsliga uppgifter om hälsa ska få hämtas in av försäkringsföretagen är utformade efter traditionell inhämtning av uppgifter på papper. Frågan är om dessa regler är tillräckliga för att

skydda den enskildes integritet när det uppkommer nya möjligheter att ta del av t.ex. journaluppgifter via nätet och genom förekomsten av olika hälsokonton.

När det gäller det hälsokonto som eHälsomyndigheten avser att erbjuda (HälsaFörMig) är tanken att enskilda ska få möjlighet att samla all information om sin hälsa på ett och samma ställe. Hälsokontot ska fungera som en tjänst som gör det möjligt för var och en att överblicka sin egen hälsoinformation över tid. Enligt eHälsomyndighetens bedömning är det individen själv som ansvarar för innehållet i HälsaFörMig och som får bestämma om någon ska ges behörighet att läsa eller hämta information. eHälsomyndigheten ska vara ansvarig för att informationen hanteras på ett säkert sätt. Myndigheten ska erbjuda tredjepart möjlighet att ansluta tillämpningar (appar) och tjänster till hälsokontot, men sedan är det individen som ska välja vilka e-tjänster han eller hon vill använda för att bearbeta och visa upp sin information.

14.4 Kommitténs samlade bedömning av området

Numera hanteras en stor del av försäkringsbolagens verksamhet med hjälp av informationsteknik. Den ökade mängden information som finns tillgänglig om enskilda personer ger försäkringsföretagen möjlighet att få bättre underlag för riskbedömning, skadebedömning och för utredning av oklara försäkringsfall. Företeelsen att med hjälp av sensorer mäta rörelse och aktivitet i bilar och hos personer ger möjlighet att göra riskbedömningen säkrare och mer individanpassad. Detta kan vara både en fördel och en nackdel beroende på hur man ser på hur risken ska fördelas i ett större kollektiv.

Den enskildes måste ge sitt samtycke för att ett försäkringsföretag ska få hämta in uppgifter om dennes hälsa från hälso- och sjukvården. Ett samtycke kan dock lämnas utan att den enskilde har tillräcklig insikt om vad samtycket innebär. Försäkringstagaren saknar dessutom i praktiken någon reell möjlighet att vägra lämna samtycke om han eller hon vill ha det aktuella försäkringsskyddet. Om det är oklart vilken ytterligare information som försäkringsföretagen har tillgång till blir det än svårare för den enskilde att förstå konsekvenserna av ett lämnat samtycke.

De nya möjligheterna att genom olika former av digitala egenmätningar lämna underlag för beräkning av försäkringspremier, t.ex. för fordonsförsäkring och personförsäkring ger upphov till nya integritetsrisker. Uppgifterna måste hanteras säkert i varje led för att det inte ska uppstå risker för obehörig spridning. Det innebär också ett stort ansvar för bolagen att inte hantera mer känsliga uppgifter än nödvändigt, eftersom tekniken i sig innefattar stora möjligheter till kartläggning av enskilda individers rörelsemönster och livsstil m.m.

När enskilda erbjuds nya möjligheter att få tillgång till uppgifter om sin hälsa genom att t.ex. kunna ta del av sin patientjournal via internet eller genom att samla sådan information på olika hälsokonton uppkommer risker för att tredjepartsintressenter vill ta del av denna information. Försäkringsföretag kan komma att vilja ta del av uppgifter om kundernas hälsa digitalt genom någon form av app knuten till ett hälsokonto, i stället för att få utskrifter ur patientjournalen. En sådan hantering förutsätter höga krav på säkerhet vid överföring av uppgifterna och ställer andra krav på den enskilde när det gäller insikter om vad överföringen av uppgifterna kan få för konsekvenser. Detta ställer i sin tur krav på företagen när det gäller ansvar för hanteringen och för information till kunderna. De risker som hör samman med användning av molntjänster uppstår också i samband med att personuppgifter kommer att behandlas av de företag som erbjuder app-tjänsterna, se vidare avsnittet om molntjänster (21.1).

Av betydelse i detta sammanhang är också att det måste finns ändamålsenliga rutiner som begränsar vilka anställda inom försäkringsföretagen som ska ha tillgång till olika uppgifter om enskilda.

Den stora mängden uppgifter som finns hos försäkringsföretagen representerar ett betydande ekonomiskt värde och skulle kunna samköras med annan information. Det kan därför finnas en risk för handel med uppgifterna. Försäkringsföretagen omfattas inte av några generella regler om tystnadsplikt. Mot denna bakgrund bedömer kommittén att det i dag finns påtagliga risker för den personliga integriteten i samband med försäkringsföretagens verksamhet.

Kommittén anser därtill att det finns särskild anledning att följa försäkringsbranschens framtida inriktning. Förutom den tekniska utvecklingen i stort, i kombination med en tänkbar förändring av branschens policyer och arbetssätt, ser kommittén en utveckling, där helt nya informationskällor uppstår, ibland som en följd av potenti-

ella försäkringstagares egna åtgärder och tillgång till delvis ny information. Den här informationen är många gånger av stort intresse för försäkringsbolagen, samtidigt som den kan vara av mycket känslig natur för den enskilde. Integritetskommittén ser en risk att den här utvecklingen ytterligare rubbar balansen mellan den enskilde försäkringstagaren och dennes försäkringsgivare.

Med tanke på den stora potentiella ökningen av nya informationskällor med känslig information och den tekniska utvecklingen i stort, bedömer kommittén att den framtida hanteringen av personuppgifter inom försäkringsverksamheten kan innefatta allvarliga risker för den personliga integriteten.

15 Bank- och kreditmarknad

Kommitténs bedömning: Det föreligger påtagliga risker för den personliga integriteten i samband med kreditprövning och rådgivning.

Det finns allvarliga risker för den personliga integriteten förknippade med användningen av kreditkort och andra digitala transaktioner.

Det finns påtagliga risker för den personliga integriteten i samband med att banker och kreditmarknadsbolag lämnar ut personuppgifter på grund av olika rapporteringskrav.

15.1 Allmänt om behandling av personuppgifter inom bank och kreditmarknadsföretag

En gång i tiden fanns riskbedömningen inbyggd i samhället. Handlaren i den lilla byn kände alla kunder och kunde avgöra vem som skulle få handla på kredit och vem som alltid skulle krävas på kontant betalning. När det sociala avståndet mellan kreditgivare och kredittagare ökade försvann denna möjlighet till en informell kreditprövning baserad på personlig kännedom om den som önskade en kredit. Dagens banker och kreditmarknadsföretag inhämtar i stället stora mängder upplysningar från bl.a. specialiserade kreditupplysningsföretag, och baserar sina bedömningar på sådan information. Behandling av personuppgifter hos kreditupplysningsföretagen behandlas närmare i kapitel 16 *Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso*.

Banksektorns intresse för data om sina kunder handlar dock inte bara om kreditbedömningar. Precis som företag i andra branscher vill bankerna ha kunskap om sina kunder för andra syften. Kunskapen blir ett underlag bl.a. i produktutveckling och marknadsföring samt styrning av verksamheten.

Banker och kreditmarknadsföretag erhåller dessutom detaljerad information om sina kunders transaktioner, t.ex. när kunderna betalar med kreditkort. Denna information sparas under viss tid, bl.a. för att kunden i efterhand ska kunna ska kunna kontrollera sitt saldo och utvecklingen av tillgångar och skulder.

Bankerna har även vissa skyldigheter enligt lag som leder till behandling av en stor mängd personuppgifter. Ett exempel på detta är att bankerna är skyldiga att kontrollera nya kunders bakgrund. Dessa kontroller ska bl.a. förhindra penningtvätt och leda till att kunder som inte är kreditvärdiga identifieras. Vidare ska vissa uppgifter om kunders tillgodohavanden och transaktioner lämnas vidare till olika myndigheter.

Det kan i teorin hävdas att enskilda kan begränsa många av dessa risker genom att aldrig söka några krediter och alltid betala med kontanter. I praktiken är det dock både svårt och dyrt för den enskilde – och i vissa fall till och med omöjligt – att göra detta. Vid betalningar av räkningar måste t.ex. mottagaren få information om vem som har gjort inbetalningen. I praktiken har den enskilde därför mycket små möjligheter att påverka personuppgiftsbehandlingen.

15.1.1 Den rättsliga regleringen

Behandlingen av personuppgifter hos banker och kreditmarknadsföretag regleras i första hand i personuppgiftslagen (1998:204). I kapitel 6 *Det grundläggande rättsliga skyddet* redogör kommittén närmare för regleringen i personuppgiftslagen.

Den allmänna regleringen i personuppgiftslagen kompletteras av vissa bestämmelser som tar sikte på just bank- och kreditmarknaden. Av såväl lagen (2004:297) om bank- och finansieringsrörelse som lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism följer t.ex. att alla som arbetar på bank har tystnadsplikt. Denna tystnadsplikt omfattar alla uppgifter som rör en bankkunds mellanhavanden med banken, oavsett om uppgiften är skriftlig eller

muntlig. Till och med uppgiften att en viss person är eller inte är kund i banken omfattas. Tystnadsplikten gäller inte endast uppgifter av ekonomisk art, utan omfattar även personliga förhållanden som t.ex. sjukdom, skilsmässa eller upprättande av testamente.

Banken får dock i vissa situationer åsidosätta tystnadsplikten och är i vissa fall till och med skyldig att göra det. Uppgifter ska t.ex. lämnas till Polis- eller Åklagarmyndigheten om undersökningsledaren begär det inom ramen för en förundersökning. Polismyndigheten ska även informeras om det, efter en analys av kundens transaktioner, föreligger omständigheter som kan tyda på penningtvätt eller finansiering av terrorism. Bankerna är även skyldiga att lämna vissa uppgifter till Skatteverket.

15.1.2 Tillsyn m.m.

Datainspektionen utövar tillsyn över bankernas och kreditmarknadsbolagens behandling av personuppgifter enligt personuppgiftslagen.

Finansinspektionen ansvarar för bl.a. tillsynen och tillståndsprövningen som rör finansiella marknader och finansiella företag samt för samordningsorganet för tillsyn enligt förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism.

Även länsstyrelserna i Skånes, Stockholms och Västra Götalands län utövar viss tillsyn över att bl.a. banker och kreditmarknadsbolag följer lagen om åtgärder mot penningtvätt och finansiering av terrorism.

15.2 Behandling av uppgifter för kreditprövning och rådgivning

15.2.1 Företeelsen

Banker och kreditmarknadsföretag samlar in stora mängder uppgifter om enskilda, för att kunna bedöma om de bör beviljas kredit. Uppgifter hämtas in från konsumenten själv samt från bl.a. kreditupplysningsföretag, Statens person- och adressregister (SPAR) och i vissa fall även från Lantmäteriverkets fastighetsregister. Om sökanden är en befintlig kund hos banken kan information även hämtas

från bankens egna interna databaser, exempelvis om hur kunden tidigare har skött relationen med banken. Det förekommer också att helt andra typer av information inhämtas och påverkar kreditbedömningen. Kreditgivare kan t.ex. vid sådan bedömning i samband med köp över internet påverkas av uppgifter om tidpunkten för köpet,[1] betalningsfrekvensen hos andra som har köpt den aktuella typen av vara,[2] eller uppgifter om återbetalningsfrekvensen hos personer som är vänner med sökanden på sociala medier.[3] Det har också förekommit att finansbolag använt data om kredittagares mobiltelefonanvändning för att göra sina kreditbedömningar.[4]

Banker och kreditmarknadsföretag samlar även in ett stort antal uppgifter om enskilda i samband med finansiell rådgivning, dvs. när en enskild får råd om hur dennes tillgångar ska placeras.

15.2.2 Det skyddande regelverket

Innan en bank beviljar en kredit ska banken enligt lagen om bank- och finansieringsrörelse pröva risken för att de förpliktelser som följer av kreditavtalet inte kan fullgöras. Banken får bevilja en kredit bara om förpliktelserna på goda grunder kan förväntas bli fullgjorda. En banks kreditprövning ska vara organiserad så att den som fattar beslut i ärendet har tillräckligt beslutsunderlag för att bedöma risken med att bevilja krediten. Vid krediter till konsumenter gäller dessutom, enligt konsumentkreditlagen (2010:1846), att kreditgivaren är skyldig att pröva om konsumenten har ekonomiska förutsättningar att fullgöra vad han eller hon åtar sig enligt kreditavtalet.

Av lagen (2003:862) om finansiell rådgivning till konsumenter följer att banken även vid finansiell rådgivning är skyldig att inhämta viss information om den enskilde. Inför rådgivningen måste banken bl.a. ställa frågor om den enskildes ekonomiska och familjeförhållanden samt om tidigare erfarenhet av finansiella placeringar, syftet

[1] Se vidare Sven Grundberg and Jens Hansegard, *Sweden's Klarna: With U.S Launch, It's all about online payment 'friction'*, Wall Street Journal 2014 samt Marc Scott, *Klarna, an Online Payment System Popular in Europe, Eyes Global Expansion*, New York Times 2014.

[2] *Big data: its power and perils*, The Association of Accountants and Financial Professionals in Business 2013.

[3] Christopher W. Surdak och Sara Agarwal, *Kreditech; The benevolent side of big data*, Finance & Development 2014.

[4] Chen, Gregory och Xavier Faz, *The potential of digital data: How far can it advance financial inclusion?*, Consultative Group to Assist the Poor 2015.

med placeringen och inställningen till risk, för att kunna anpassa rådgivningen efter konsumentens önskemål och behov. Banken är även skyldig att avråda från åtgärder som inte kan anses lämpliga med hänsyn till konsumentens behov, ekonomiska förhållanden eller andra omständigheter. De råd som lämnas ska dessutom dokumenteras.

Det anförda innebär inte att banker och kreditmarknadsbolag får behandla vilka uppgifter som helst, eller att behandlingen får göras hur som helst. Enligt personuppgiftslagen måste personuppgifter som behandlas vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Datainspektionen har gjort bedömningen att uppgifter om avskrivna och överlåtna fordringar inte är adekvata eller relevanta att använda för kreditprövning när uppgifterna är äldre än tre år.[5]

Alla anställda vid banker och kreditmarknadsbolag har dessutom, som tidigare nämnts, en långtgående tystnadsplikt.

15.2.3 Risker för den personliga integriteten

Med teknikgenombrott som internet och big data har möjligheterna att basera kreditbedömningar på andra uppgifter än tidigare ökat markant. Andra data än de som finns hos kreditupplysningsföretagen kan säga mycket – i vissa fall kanske till och med mer – om en individs kreditvärdighet. Aktörer som gör riskbedömningar har därför ett intresse av att få tillgång till information som kan erhållas genom den kartläggning som görs om enskilda individer, bl.a. på internet. Sådan information kombinerat med verktyg för dataanalys gör det möjligt för en kreditgivare att minska sina risker.

Denna utveckling innebär flera risker för den personliga integriteten. En del i detta är att företag, t.ex. banker och kreditmarknadsföretag, typiskt sett har tillgång till en stor mängd information om sina kunder i de interna systemen. Det kan t.ex. handla om uppgifter om sparat kapital, genomförda transaktioner och tidigare tagna krediter, men även exempelvis uppgifter om ifall en viss kund väljer att kommunicera med banken genom personliga besök, via telefon eller

[5] Datainspektionens beslut den 9 juni 2014, dnr 1822-2013 och 1826-2013.

via internet. När nya analysverktyg används för att kombinera denna information med information från olika externa aktörer, kan man erhålla detaljerad information om den enskilda kunden.

Tidigare handlade den externa informationen i huvudsak om uppgifter från traditionella kreditupplysningsföretag. Teknikutvecklingen har dock medfört att det exempelvis via sociala medier går att få en bild av en persons sociala nätverk, men också om livssituation och konsumtionsvanor. Det finns också en växande handel med kunddata via företag som specialiserat sig på handel med personuppgifter av varierande slag, s.k. data brokers.

När förutsättningarna förändras för hur en kreditbedömning genomförs, får det också konsekvenser för kredittagarna. Redan 2009 uppmärksammade amerikanska ABC ett fall där en man plötsligt fick sin kontokortskredit sänkt från 10 800 till 3 800 dollar, trots att hans Fico-ranking (en av de modeller för kreditprövning som används i USA) var väldigt hög. Det visade sig att den sänkta krediten var en konsekvens av att han hade handlat i en butik där många andra kreditkortsinnehavare med dålig återbetalningshistorik brukade handla.[6]

Det finns även exempel från Sverige som visar att kreditprövning gjorts på ett sätt som varken varit objektivt eller transparent. Under våren 2013 förekom t.ex. rapportering i svensk media om att en svensk storbank hade fört ett register (en s.k. svart lista) över personer som bedömdes vara olämpliga som bankkunder samt att banken i registret använde epitet som ”skojare”, ”ekonomisk vettvilling”, ”känd skumraskfigur”, ”tvivelaktig mäklare”, ”gangsterrevisor” och ”rövarflicka”.[7] Beträffande en person i registret ska det ha stått ”Brott. Narkotikabrott. Dömd 1987. Obeståndsgäldenär”.

Det har även förekommit användning som, beroende på omständigheterna, kan vara både positiv och negativ för den enskilde. Nya metoder för kreditbedömning kan i vissa fall resultera i att en kredit beviljas trots att en mer traditionell prövning hade utmynnat i ett avslag. Detta är i bästa fall positivt för den enskilde. Det har även förekommit att banker som har avslagit en ansökan om kredit har sålt sina uppgifter om kunden till en annan långivare, som har kon-

[6] Chris Cuomo m.fl., ‘*GMA*’ *Gets Answers: Some Credit Card Companies Financially Profiling Customers*, abc NEWS 2009.

[7] Se t.ex. Joel Dahlberg och Carolina Neurath, *Nordea bluffade om hemliga kundregistret*, Svenska dagbladet 2015, och Stockholm TT, Bankerna förnekar svarta listor, Svenska dagbladet 2013.

taktat kunden och erbjudit denne ett lån mot högre ränta.[8] En sådan överföring får dock inte göras utan att banken först inhämtar den enskildes samtycke.

Det finns även andra aspekter. Banker och kreditmarknadsföretag kan precis som alla andra utnyttja nätets möjligheter till individanpassade erbjudanden. Som exempel på detta kan nämnas att individer som efter dataanalys placerats i målgruppen för högräntelån kan exponeras för annonser med erbjudanden om sådana lån.

Möjligheterna att upptäcka samband mellan olika data kan också användas för att försöka kringgå förbud mot viss behandling av personuppgifter. I USA förekom t.ex. länge s.k. redlining, vilket innebar att kreditgivare ägnade sig åt väldigt grova generaliseringar i sin riskbedömning; till boende i vissa bostadsområden – som markerades med röda linjer på en karta – skulle inga krediter ges. Med big data-verktyg har det öppnats möjligheter att uppnå samma effekt som med hjälp av redlining, som i dag är förbjuden. Går det t.ex. att använda enskildas musiksmak för att bedöma kreditrisken? Weblining har börjat användas som term när en individs digitala fotspår används på detta sätt.

15.3 Kreditkort och transaktioner över internet

15.3.1 Företeelsen

Konsumenter betalar allt oftare med bank- eller kreditkort. Det gäller i synnerhet vid köp över internet. Vid betalningar över internet eller med kort får banken eller kreditmarknadsföretaget kontinuerligt detaljerad information om kundernas transaktioner. Denna information sparas under viss tid, bl.a. för att kunden i efterhand ska kunna kontrollera sitt saldo och förändringar av tillgångar eller skulder.

Många banker och kreditmarknadsföretag tillhandahåller dessutom appar för sina kunder. I dessa appar kan kunderna ta del av vissa uppgifter, t.ex. saldon, transaktioner, aktieinnehav och uppgifter om lån. Via apparna kan kunderna oftast också genomföra vissa transaktioner, såsom överföringar och betalningar. I regel kan kunderna

[8] Se t.ex. Carolina Neurath, *FI utreder bankernas affärer med kunddata*, och *Storbanker säljer ratade kunder vidare*, Svenska dagbladet 2013.

även ta del av denna typ av uppgifter, och utföra vissa transaktioner, över internet. Det går även i många fall att ansöka om lån eller beställa en e-legitimation över internet. Lån kan till och med sökas via SMS hos vissa kreditgivare.

15.3.2 Det skyddande regelverket

Alla anställda vid banker och kreditmarknadsbolag har, som tidigare nämnts, en långtgående tystnadsplikt. Vidare uppställer personuppgiftslagen krav på lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,

b) vad det skulle kosta att genomföra åtgärderna,

c) de särskilda risker som finns med behandlingen av personuppgifterna, och

d) hur pass känsliga de behandlade personuppgifterna är.

Av Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse (FFFS 2015:15) följer att bl.a. banker genast bör rapportera till Finansinspektionen om det inträffar sådana händelser som kan medföra att företagets ekonomiska förutsättningar ändras, så att det inte kan uppfylla sina åtaganden mot kunder. Vidare anges att företag bör rapportera händelser som kan medföra att ett större antal kunder orsakas betydande ekonomisk skada, och händelser som kan medföra en väsentlig ryktesförlust för företaget. De händelser som avses är t.ex. att information som lämnas vid kundtransaktioner är felaktig eller bristfällig, att kundtransaktioner hanteras på ett felaktigt eller bristfälligt sätt, att fel uppstår i tekniska system, eller att interna eller externa regler överträds.

15.3.3 Risker för den personliga integriteten

Inledning

Vid användning av kreditkort och transaktioner över internet får bl.a. banker och kreditmarknadsföretag tillgång till detaljerade uppgifter som kan vara känsliga från ett integritetsperspektiv. När kunderna ges en möjlighet att komma åt sådana uppgifter och utföra transaktioner via appar eller internet, finns en risk att även obehöriga kan utföra sådana åtgärder.

Kontant betalning minskar till förmån för betalning med kreditkort eller andra betalningar över internet. En risk som är förknippad med denna utveckling är att möjligheterna att betala utan att skapa elektroniska spår försvåras alltmer.

Bankers och kreditmarknadsbolags behandling av transaktionshistorik

Vid betalning med konto- eller kreditkort lagras transaktionerna i olika register. Görs inköpen via internet lämnas även digitala spår.

Med hjälp av uppgifter om den enskildes inköpsmönster går det att dra många slutsatser om dennes liv och personlighet.

Register som innehåller uppgifter om inköp är inte sällan avsedda att vara anonymiserade, exempelvis genom att varje användare anges med ett unikt ID-nummer. Det finns dock undersökningar som visar att sådan anonymisering inte alltid fungerar som det är tänkt. Amerikanska forskare har t.ex. undersökt ett kreditkortsregister som skulle vara anonymiserat och kunnat namnge 90 procent av de 1,1 miljoner personer som fanns i registret. Enligt dessa forskare var det tillräckligt med två fakta om en person i en databas med 1,1 miljoner ”anonymiserade” personer, för att med mer än 50 procents sannolikhet kunna peka ut rätt person i databasen. När en person väl är avanonymiserad är det ofta möjligt att följa personens handlingar under en längre tidsperiod och se var personen befunnit sig och vad denne har gjort eller inhandlat osv. Det gäller särskilt om dessa data

kombineras med information från en annan källa, exempelvis sociala medier. Uppgifter av detta slag sprids också allt oftare mellan företag och myndigheter.[9]

Transaktionshistorik är även intressant för andra än kreditgivare och därför på väg att bli en handelsvara. I USA har det t.ex. genomförts försök där vårdgivare med hjälp av big data-verktyg har analyserat inköpsvanorna hos två miljoner människor, i syfte att identifiera högriskpatienter innan de blir sjuka. Man kan exempelvis bedöma sannolikheten för att en astmapatient ska uppsöka akutsjukvård utifrån faktorer som cigarettinköp, luftföroreningar och uppgifter om personen har hämtat ut astmamedicin på apoteket, eller sannolikheten för att en person ska drabbas av en hjärtattack, bl.a. utifrån vilken sorts mat personen har inhandlat och om han eller hon är medlem i ett gym.[10]

Bankappar och internetbank

Möjligheten att kontrollera saldon och genomföra transaktioner med hjälp av bankappar och internetbank är mycket smidig och kan vara tidsbesparande för den enskilde. Det kan också innebära sänkta transaktionskostnader för banken.

Det kan dock medföra stora risker för den enskildes personliga integritet om någon obehörig får tillgång till t.ex. uppgifter om konton, transaktioner med namn på mottagaren eller avsändaren och om skuldsättning. Uppgifterna kan användas till att kartlägga inte bara stora delar av en persons ekonomiska förhållanden, utan även var denne har befunnit sig och dennes inköpsvanor. Uppgifter om transaktioner kan dessutom innehålla känsliga uppgifter i personuppgiftslagens mening, t.ex. genom att avslöja den enskildes kontakter med hälso- och sjukvården.

Särskilt med tanke på att appar ofta används på offentliga platser finns en ökad risk för att någon obehörig lyckas komma åt inloggningsuppgifterna. Denne skulle därefter, genom att enkelt ladda ner

[9] Linus Brohult, Så avslöjas dina ”hemliga” uppgifter, svt.se 2015; de Montjoye m.fl, *Unique in the shopping mall: On the reidentifiability of credit card metadata*, Science 2015.

[10] Shannon Pettypiece och Jordan Robertson, *Hospitals are mining patients' credit card data to predict who will get sick*, Bloomberg Business 2014.

bankens app till sin egen smarta telefon, kunna logga in i appen och obehörigen ta del av en stor mängd uppgifter, utan att den behörige användaren märker det.

Datainspektionen har granskat ett antal bankappar och gjort bedömningen att flera av de uppgifter som man fått åtkomst till via apparna har ett så högt skyddsvärde att åtkomsten till dessa uppgifter ska föregås av stark autentisering, för att säkerställa att rätt person gör inloggningen.[11] Stark autentisering kan åstadkommas på flera sätt, t.ex. e-legitimation.

I detta sammanhang kan också nämnas en ny typ av tjänst som lanserats i form av s.k. privatekonomiappar. Syftet med tjänsten är att ge användaren överblick över sin ekonomi. Appen kopplas till användarens internetbank, genom att en personlig bankkod anges. Sedan samlas uppgifter om transaktioner och saldon in för att skapa diagram över användarens konsumtion. Att lämna ut bankkoder till en tredje part kan dock innebära stora risker för att bankuppgifter hamnar i fel händer.[12]

Identitetsstölder och bedrägerier

När någon använder en annan persons identitet för att begå brott brukar man tala om identitetsstöld. Ett typiskt exempel på identitetsstöld är att någon beställer varor, skaffar sig lån eller begår andra bedrägerier i en annan persons namn. I vissa fall föregås brotten av omsorgsfull planering t.ex. på det sättet att gärningsmannen beställer ett kreditkort eller en e-legitimation i någon annans namn och därefter stjäl det kreditkort, uppgift om koder eller liknande som skickas till den förmente beställarens hemadress. Ibland begär gärningsmannen adressändring för brottsoffret och får på så sätt tillgång till hans eller hennes post. Därefter utnyttjas kreditkortet, e-legitimationen eller motsvarande för att exempelvis köpa varor eller ta upp lån. Det är som regel först när krav på obetalda varor eller återbetalning av lån börjar dyka upp, som den vars identitet har utnytt-

[11] Datainspektionens beslut den 11 september 2013, dnr 1612-2011 och 1613-2011.
[12] Se Josefin Jacobsson, *Få budgetkoll med en app*, Svenska dagbladet 2014, samt Susanna Nordenhem och Martin Hansson, *Säkerhetsexpert varnar för ekonomiappar*, Testfakta 2014.

jats, upptäcker vad som har inträffat. Under mellantiden kan varor till sammanlagt stort värde ha lämnats ut eller lån ha tagits till avsevärda summor.[13]

Problemet med stöld av identiteter uppges ha vuxit sig mycket stort under senare år. Det är framför allt ändrade köpvanor och betalningsvanor som har lett till att olovlig användning av annans identitetsuppgifter ökar. Både köp, beviljande av lån, betalningar och kontakter med myndigheter, görs numera via internet eller telefon, i stället för öga mot öga. Detta ökar avsevärt möjligheterna att utge sig för att vara någon annan. Gärningsmännen drar också nytta av att bedrägerioffret – t.ex. en kreditgivare – inte har samma möjligheter som vid ett personligt sammanträffande att bilda sig en uppfattning om den person som han eller hon gör affärer med. Det är också enkelt att skaffa ett SMS-lån i någon annans namn om man känner till hans eller hennes personnummer, eftersom företagen tillåter att detta görs enbart via mobiltelefonen.[14]

Ett grundproblem är, enligt uppgifter från bl.a. Bankföreningen och Polismyndigheten, att de svenska legitimationerna, som det finns många varianter av, är lätta att förfalska. Det finns exempel på att bedragare kapat kända finansmäns identiteter, skaffat e-legitimationer i deras namn och sedan tagit ut stora belopp från deras konton.[15] Ett annat uppmärksammat exempel är att s.k. hackers i april 2011 stal personlig information för hundra miljoner användare från Sony Playstation Network. Enligt Sony hade tio miljoner användare bl.a. sina kreditkortsuppgifter på servern där dataintrånget begicks.[16]

En företeelse som är starkt förknippad med identitetsstöld är s.k. phishing, som på svenska kallas nätfiske eller lösenordsfiske. Nätfiske utförs som regel genom att någon skickar e-postmeddelanden – som ofta ser ut att komma från en bank eller ett kreditkortsföretag – och som innehåller en uppmaning att logga in snarast möjligt och en länk till en falsk webbsida med inloggningsformulär. E-postmeddelandet kan också vara utformat så att det ser ut att komma från t.ex. ett företags supportavdelning eller en myndighet. Det förekommer också att gärningsmännen skapar falska webbsidor

[13] Egendomsskyddsutredningen betänkande *Stärkt straffrättsligt skydd för egendom*, SOU 2013:85, s. 191.
[14] SOU 2013:85 s. 192 f.
[15] Daniel Goldberg, *Den stora blåsningen*, Di Digital 2015.
[16] Waldemar Ingdahl, *Tiden mogen att begrava kreditkortet*, Svenska dagbladet 2011.

utan att skicka ut e-postmeddelanden, i förhoppningen om att enskilda ska logga in på fel hemsida. Metoden används ibland också på det sättet att det görs ett massutskick, som skenbart kommer från ett företag med många kunder, och som underrättar mottagaren om att han eller hon tyvärr har debiterats två gånger för samma räkning och där man efterfrågar kontonummer och andra uppgifter för att kunna sätta in det felaktigt debiterade beloppet på kundens konto. Syftet är oftast att lura innehavare till bankkonton eller kreditkort att lämna ut kreditkortsnummer, lösenord eller annan känslig information till den som skickat meddelandet. Gärningsmannen vill komma åt uppgifterna om bankkonton och kreditkort för att kunna föra över pengar från kontona eller kunna utnyttja kreditkortsnummer för köp via internet.[17]

En annan typ av bedrägerier som enligt bl.a. Swedbank ökar är det som kallas för Facebook-bedrägerier. Vid ett Facebook-bedrägeri kapar bedragaren ett konto på Facebook för att därefter via meddelanden på sajten lura den kapades vänner att exempelvis lämna ifrån sig inloggningsuppgifter till nätbanken.[18]

När någon annans identitet olovligen används vid ett bedrägeri kan konstateras att dagens reglering ger straffrättsligt skydd mot själva bedrägeriet. Detsamma gäller brukandet av falska och osanna handlingar, t.ex. handlingar som ger sken av att gärningsmannen har en viss identitet som tillhör någon annan. Något straffrättsligt skydd mot användningen av någon annans identitet i sig finns däremot inte ännu. Egendomsskyddsutredningen lämnade i sitt betänkande[19] föreslag om att olovlig användning av andras identitetsuppgifter ska straffbeläggas som ett särskilt brott, benämnt identitetsintrång. Syftet med straffbestämmelsen är att ge skydd mot den integritetskränkning som olovlig användning av annans identitetsuppgifter innebär och att ge den drabbade bättre möjligheter att ta tillvara sin rätt. Den 17 mars 2016 lämnade regeringen ett förslag till riksdagen om en sådan lagstiftning.[20]

---

[17] SOU 2013:85 s. 193.

[18] *Bedrägerier*, information på Swedbanks webbplats 2015-11-05 – https://www.swedbank.se/foretag/sakerhet/sakerhet-och-vanliga-bedragerier/bedragerier/index.htm#!/

[19] SOU 2013:85.

[20] Regeringens proposition *Straffrättsligt skydd mot olovlig identitetsanvändning*, prop. 2015/16:150.

Ett område där banker och kreditmarknadsbolag har varit framgångsrika när det gäller dataanalys är just i kampen mot kortbedrägerier. Genom att analysera ett stort antal faktorer av en transaktion kan it-systemen hitta de kortköp som förefaller vara bedrägerier. I en artikel i Wall Street Journal 2013 berättade en företrädare för Visa att företaget då baserade sina analyser på 500 olika aspekter av en korttransaktion, vilket varje år stoppar bedrägeriförsök för miljarder dollar.[21]

Inom ramen för ett nordiskt samarbete har banker utväxlat uppgifter om IP-adresser som förekommit i samband med intrångsförsök. Syftet med behandlingen har inte varit att utpeka innehavaren av IP-adressen som misstänkt brottsling, utan att förhindra angrepp mot bankerna och deras kunder. Bankerna har inte själva haft möjlighet att identifiera personen som står bakom IP-numret. Datainspektionen har därför gett tillstånd till sådant utbyte av information, trots att grundprincipen är att endast myndigheter får behandla personuppgifter om lagöverträdelser som innefattar brott.[22]

15.4 Behandling av uppgifter för att uppfylla rapporteringskrav m.m.

15.4.1 Företeelsen

Inledning

Banker och kreditmarknadsbolag är i viss mån skyldiga att lämna ut uppgifter till olika myndigheter. Det finns bl.a. en skyldighet att lämna ut uppgifter till Polis- eller Åklagarmyndigheten under en pågående förundersökning. Det finns även en skyldighet att lämna uppgifter till Kronofogdemyndigheten i samband med att den myndigheten undersöker om en enskild har tillgångar som kan utmätas eller beläggas med kvarstad. Vidare finns också en skyldighet att lämna sedvanliga kontrolluppgifter till Skatteverket.

[21] Steve Rosenbush, *Visa Says Big Data Identifies Billions of Dollars in Fraud*, Wall Street Journal 2013.
[22] Datainspektionens beslut den 18 mars 2008, dnr 1402-2007.

Av särskilt intresse i detta sammanhang är dock de särskilda skyldigheter som banker och kreditmarknadsbolag har i arbetet för att förhindra penningtvätt och finansiering av terrorism samt inom ramen för det internationella skatterättsliga samarbetet.

Åtgärder för att förhindra penningtvätt och finansiering av terrorism

Den verksamhet som banker och kreditmarknadsbolag bedriver kan utnyttjas för omfattande penningtvätt och finansiering av terrorism. Det kan handla om att föra in tillgångar från brottslig verksamhet – t.ex. rån, skattebrott, narkotikahandel, prostitution, trafficking eller människohandel – i det lagliga, finansiella systemet för att dölja den brottsliga källan, eller för insamling, tillhandahållande eller mottagande av tillgångar i syfte att de ska användas eller med vetskap om att de är avsedda att användas för terrorism. Det finns därför ett behov av åtgärder som effektivt motverkar att bankernas tjänster används för sådan verksamhet.

Inom FN fattas för medlemsstaterna bindande beslut om sanktioner mot vissa organisationer, personer, grupper och företag, för att motverka internationell terrorism. I EU genomförs nämnda sanktioner genom gemensamma ståndpunkter och EU-förordningar. Finansiella företag i EU är följaktligen skyldiga att respektera dessa beslut. Företagen ska bl.a. informera Finansinspektionen om konton och belopp som frysts enligt sanktionerna och meddela förändringar för dessa konton.

Därutöver uppställer lagen om åtgärder mot penningtvätt och finansiering av terrorism krav på företag inom EU att vidta åtgärder för att förhindra att den egna verksamheten utnyttjas för penningtvätt. Enligt lagen, som bygger på EU:s tredje penningtvättsdirektiv, ska finansiella företag ha rutiner för att säkerställa att de har tillräcklig kunskap om sina kunder. En god kundkännedom anses förutsätta att företaget identifierar sin kund på ett säkert sätt och att pågående affärsförbindelser fortlöpande följs. Åtgärderna ska anpassas efter risken för att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism.

Bankernas åtgärder för att leva upp till kravet på kundkännedom kan t.ex. innebära att man, inför att en affärsförbindelse inleds med en ny kund, hämtar in grundläggande uppgifter om namn, person-

nummer, adress m.m. från personen själv samt att banken kontrollerar personen mot EU:s sanktionslista och den amerikanska OFAC-listan. Det sistnämnda är en förteckning över USA:s sanktioner mot s.k. Specially Designated Nationals and Blocked Persons (SDN), vilken administreras av en myndighet under USA:s finansdepartement som heter Office of Foreign Assets Control (OFAC). Även den listan måste respekteras av svenska banker och kreditmarknadsbolag som t.ex. avser att ingå avtal med ett amerikanskt finansiellt institut.

I de fall personen är föremål för skärpta åtgärder för att uppnå kundkännedom görs även en kontroll i databasen Worldcompliance Global PEP List (Worldcompliance). I samband med detta kontrolleras om personen är i politiskt utsatt ställning, en s.k. Politically Exposed Person (PEP). En PEP är en person som genom sin position och sitt inflytande anses inneha en ställning som i sig utgör en risk för att utnyttjas för bl.a. mutbrott och andra former av korruption och i förlängningen penningtvätt, liksom för aktiviteter som kan relateras till finansiering av terrorism.

Banker och kreditmarknadsbolag måste också granska sina transaktioner för att kunna upptäcka misstänkta transaktioner. Vid misstanke ska detta anmälas till Finanspolisen (en sektion inom Nationella operativa enheten vid Polismyndigheten). Uppgifter som identifierats i samband med kontrollerna bevaras i dessa fall i bankernas penningtvättsregister.

Om en person blir kund sparar banken loggar över de kontroller som gjorts. Om banken inte lyckas uppnå kundkännedom får en affärsförbindelse inte etableras eller en transaktion inte utföras med kunden. Om personen nekas att bli kund rapporteras detta till Finanspolisen.

Skatterättsligt samarbete

Foreign Account Tax Compliance Act (FATCA) är en amerikansk lag från år 2010 som ålägger finansiella institut, dvs. bl.a. banker och kapitalmarknadsföretag, i hela världen att identifiera finansiella konton som innehas av amerikanska personer och rapportera tillgångar och inkomster på sådana konton till den amerikanska federala skattemyndigheten (Internal Revenue Service, IRS). Syftet med FATCA

är att IRS ska få tillgång till information om amerikanska personers kapitaltillgångar och kapitalinkomster som förvaltas av eller betalas till icke-amerikanska finansiella institut. I vissa fall ska de finansiella instituten också innehålla skatt för IRS räkning. Finansiella institut som inte medverkar i detta samarbete riskerar att en skatt om 30 procent innehålls på alla betalningar från USA.

För att underlätta för svenska finansiella institut att medverka i samarbetet och lämna dessa uppgifter till IRS har Sverige ingått ett avtal med USA, det s.k. FATCA-avtalet. Avtalet innebär i korthet att dessa företag årligen lämnar kontrolluppgifter till Skatteverket, som vidarebefordrar informationen till IRS. I kontrolluppgifterna ska bl.a. lämnas information om kontohavarna och uppgifter om saldon, inkomster samt ersättningar från försäljningar och inlösen av värdepapper.

Vidare har det inom OECD tagits fram en standard för automatiskt utbyte av upplysningar om finansiella konton. Denna globala standard, som även har antagits inom EU,[23] bygger på modellen för de bilaterala FATCA-avtalen med USA. Standarden innebär att finansiella institut identifierar utländska kontohavare och lämnar information om deras tillgångar och kapitalinkomster till sina respektive nationella skatteverk. Informationen överförs därefter till det land där kontohavaren har hemvist.

15.4.2 Det skyddande regelverket

I lagen om åtgärder mot penningtvätt och finansiering av terrorism finns ett kapitel med bestämmelser om behandling av personuppgifter. Där finns bl.a. bestämmelser om behandling av känsliga personuppgifter och om tystnadsplikt. I de fall annat inte följer av dessa bestämmelser är personuppgiftslagen tillämplig. Det innebär bl.a. att det är förbjudet att till tredje land föra över personuppgifter som är under behandling, om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredje land. Frågan om en skyddsnivå är adekvat ska bedömas med hänsyn till samtliga omständigheter som

[23] Se rådets direktiv 2011/16/EU av den 15 februari 2011 om administrativt samarbete i fråga om beskattning, senast ändrat genom rådets direktiv 2014/107/EU av den 9 december 2014. Se även prop. 2015/16:29, *En global standard för automatiskt utbyte av upplysningar om finansiella konton*.

har samband med överföringen. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet.

FATCA-avtalet innehåller bestämmelser som begränsar hur informationen får användas i det land som tar emot uppgifterna. Begränsningarna innebär bl.a. att informationen som IRS erhåller från Sverige bara får användas för beskattningsändamål i USA.

Enligt personuppgiftslagen är det förbjudet för andra än myndigheter att behandla uppgifter om lagöverträdelser som innefattar brott. Datainspektionen får dock i föreskrifter eller enskilda fall meddela undantag från detta förbud. Sådana undantag har meddelats bl.a. när det gäller bankers löpande kontroll av kunddatabaser mot den s.k. OFAC-listan.[24]

15.4.3 Risker för den personliga integriteten

Penningtvätt och finansiering av terrorism är internationella problem som skadar förtroendet för det finansiella systemet och i förlängningen hela samhället. Det finns därför ett starkt behov av åtgärder för att motverka sådan verksamhet. Detsamma gäller i stor utsträckning för skatteflykt.Vid sanktioner mot enskilda finns i princip alltid viss risk att helt oskyldiga personer felaktigt förknippas med en person med samma namn som förekommer på sanktionslistorna. Just detta problem kan dock motverkas genom att banker och andra har rutiner för att hindra sådan sammanblandning av personer. En enskild kan dock även av andra skäl bli felaktigt placerad på en sanktionslista. Det medför stora konsekvenser för den enskilde som har obefintliga möjligheter att påverka listningen.

Vidare innebär den mycket breda internationella uppslutningen kring OECD:s standard för automatiskt utbyte av upplysningar om finansiella konton ett globalt genombrott för automatiskt informationsutbyte i skatteärenden, och därmed för arbetet mot skatteundandragande och skattefusk. Samtidigt innebär i princip allt internationellt informationsutbyte vissa risker från ett integritetsperspektiv. Det uppkommer bl.a. frågor om hur överskottsinformation hanteras

[24] Datainspektionens beslut den 16 september 2010, dnr 589-2010.

i systemen och om andra länder kan garantera att informationen inte används för otillåtna ändamål eller lämnas vidare. Sekretesskyddet hos den utländska mottagaren kan t.ex. vara svagare än i Sverige.

Problematiken kan illustreras med följande exempel. Världens banker genomför miljontals internationella transaktioner varje dag. Nästan alla dessa transaktioner görs genom Society for Worldwide Interbank Financial Telecommunication (Swift), som är ett belgiskt bolag. Tidigare sparade Swift alla uppgifter om dessa transaktioner, dvs. om vem som överförde pengar till vem, på servrar i såväl EU som USA. Efter den 11 september 2001 beslutade dock amerikanska myndigheter att ålägga Swift att ge dem tillgång till uppgifterna, för att myndigheterna skulle kunna spåra misstänka överföringar.[25] När detta uppmärksammades och bl.a. Artikel 29-gruppen framförde skarp kritik, beslutade Swift att flytta den lagring som tidigare hade gjorts i USA till Schweiz.[26]

Den omständigheten att visst informationsutbyte, exempelvis utbytet enligt FATCA, kan omfatta en stor mängd uppgifter ökar risken för integritetsintrång. Skattskyldighet i USA föreligger om man är medborgare i USA, vilket även innefattar personer med dubbelt medborgarskap, eller ”tax resident” i landet (t.ex. en icke-amerikansk medborgare som har uppehålls- och arbetstillstånd, s.k. grönt kort, i USA). Detta innebär att även amerikanska medborgare som flyttat ut ur landet eller aldrig ens har bott där, liksom icke-amerikaner som flyttat hem från USA men som fortfarande har grönt kort, är skatt- och deklarationsskyldiga i USA, trots att de betalar skatt i det nya hemlandet. Informationsskyldigheten enligt FATCA omfattar alltså alla dessa personer.

Det måste dock även vägas in i bedömningen hur svenska kreditinstitut och andra aktörer påverkas om man ställer sig utanför internationella samarbeten. Det kan t.ex. medföra att affärstransaktioner måste avvecklas eller att utländska myndigheter vidtar åtgärder.[27]

[25] Se t.ex. Datainspektionens tidning Magazin Direkt, nr 4 år 2006, s. 10.
[26] Se t.ex. Datainspektionens tidning Magazin Direkt, nr 4 år 2007, s. 6.
[27] Datainspektionens beslut den 16 september 2010, dnr 589-2010.

15.5 Kommitténs samlade bedömning av området

Numera hanteras en stor del av bankernas och kreditmarknadsföretagens verksamhet med hjälp av informationsteknik. Användningen av sådan teknik har också gett dessa företag tillgång till nya typer av uppgifter, som kan användas vid exempelvis kreditprövningar. Detta är på många sätt en positiv utveckling och har bl.a. lett till effektivitetsvinster. Utvecklingen har dessutom medfört en rad förbättringar för kunderna, inte minst när det gäller tillgänglighet. Ett exempel på detta är möjligheterna att använda appar och internetbank för många transaktioner.

Samtidigt gäller de uppgifter som bankerna och kreditmarknadsbolagen behandlar i stor utsträckning enskildas personliga och ekonomiska förhållanden. Sådana uppgifter är normalt att anse som integritetskänsliga. Ett uttryck för detta är att uppgifterna omfattas av tystnadsplikt eller sekretess. Den information om enskilda som finns hos dessa banker och kreditmarknadsbolag ger stora möjligheter att göra en detaljerad kartläggning av en persons liv. Med utgångspunkt från en individs inköpsmönster kan det vara möjligt att dra slutsatser om dennes personlighet. Det har också visat sig att det även i anonymiserade uppgiftssamlingar kan vara lätt att identifiera enskilda individer.

I detta kapitel har vi analyserat risker för integritetsintrång som hör ihop med bankers och kreditmarknadsbolags behandling av personuppgifter i samband med:

– kreditprövning och rådgivning,
– enskildas användning av kreditkort och transaktioner på internet, och
– i samband med rapporteringskrav.

Kreditprövning och rådgivning

Möjligheten att basera kreditprövning på information som normalt inte behandlas hos kreditupplysningsbolagen, exempelvis uppgifter om inköpsmönster, ökar risken för att prövningen blir mindre transparent och för att ovidkommande faktorer beaktas. Om kreditgivare samlar in uppgifter om sina kunder utan att kunderna informeras om

vilka uppgifter som behandlas, förlorar den enskilde också möjligheten att kontrollera uppgifterna och att begära rättelse av eventuella felaktiga uppgifter. De s.k. svarta listor som uppges ha förekommit hos en av storbankerna illustrerar detta problem.

Den stora mängden uppgifter som finns hos banker och kreditmarknadsbolag representerar dessutom ett betydande ekonomiskt värde, och kan samköras med annan information. Det finns av dessa skäl en risk för handel med uppgifterna, trots sekretess. Som framgått ovan har det också förekommit att banker har fört vidare uppgifter om kunder som nekats lån.

Av betydelse i detta sammanhang är också att det måste finns ändamålsenliga rutiner som begränsar vilka inom banken eller kreditmarknadsföretaget som ska ha tillgång till olika uppgifter. Huvudregeln bör vara att endast den som behöver uppgifterna i sitt arbete ska ha tillgång till dem. Såvitt framkommit tillämpar banker och kreditgivare allt oftare olika former av åtkomstkontroll inom verksamheten.

I sin kreditgivnings- och rådgivningsverksamhet behandlar banker och kreditgivare en stor mängd uppgifter om en stor del av befolkningen. Uppgifter som sammantaget kan upplevas som närgångna. Det är svårt för en enskild person att veta vilka uppgifter som ligger till grund för en kreditbedömning. Uppgifterna har ett ekonomiskt värde. Kommittén bedömer därför att det föreligger påtagliga risker för den personliga integriteten i samband med kreditprövning och rådgivning.

Kreditkort och transaktioner på internet

När det gäller kreditkort och transaktioner på internet konstaterar kommittén att de digitala spår som skapas genom sådana transaktioner gör det möjligt att kartlägga enskilda personers konsumtionsmönster på ett närgånget sätt. Sådana uppgifter har ett högt kommersiellt värde och kan komma att användas på sätt som den enskilde inte kan förutse. När det gäller användningen av banktjänster som internetbank och olika appar konstaterar kommittén att det är nödvändigt med hög säkerhet vid sådan behandling på grund av risken

för att närgångna uppgifter blir åtkomliga för obehöriga. Digitala banktjänster är också förknippade med risken för den enskilde att bli utsatt för identitetsstölder.

Behandling av personuppgifter i samband med användning av kreditkort och andra transaktioner på internet gör det möjligt att kartlägga enskilda personers konsumtionsmönster. Det handlar om stora mängder uppgifter om i stort sett alla människor. Företeelsen är förknippad med risker för bedrägerier och identitetsstölder. Kommittén bedömer därför att det finns allvarliga risker för integritetsintrång förknippade med användningen av kreditkort och andra digitala transaktioner.

Rapporteringskrav

Det bör vidare understrykas att bankernas och kreditmarknadsbolagen har fått en roll i arbetet mot bl.a. penningtvätt och mot finansiering av terrorism som innebär ett stort avsteg från principen att endast myndigheter får behandla uppgifter om lagöverträdelser som innefattar brott. I arbetet mot sådan brottslighet finns också en risk att helt oskyldiga personer placeras på olika former av sanktionslistor, vilket kan få stora konsekvenser för den enskilde. Den enskilde har i praktiken inte heller någon möjlighet att påverka sådana åtgärder.

Vid spridning av uppgifter till andra länder tillkommer problemet att det i praktiken inte längre går att kontrollera hur uppgifterna används och i övrigt behandlas. De amerikanska myndigheternas behandling av Swift-transaktionerna är ett exempel på detta.

Riskerna i samband med hantering av personuppgifter på grund av olika rapporteringskrav består bl.a. i att uppgiftssamlandet kan påverka helt oskyldiga. Det kan vara svårt att kontrollera uppgifter som lämnats ut internationellt. Men området är reglerat och rimligen drabbas bara ett begränsat antal personer. Kommittén bedömer därför att det finns påtagliga risker för den personliga integriteten i samband med att banker och kreditmarknadsbolag lämnar ut personuppgifter på grund av olika rapporteringskrav.

16 Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso

Kommitténs bedömning: Det finns vissa risker för den personliga integriteten i kronofogdemyndighetens verksamhet.

Det föreligger allvarliga risker för den personliga integriteten i kreditupplysningsföretagens verksamhet

Det föreligger vissa risker för den personliga integriteten på grund av behandling av personuppgifter i inkassobolagens verksamhet.

16.1 Inledning

I Kronofogdemyndighetens verksamhet liksom i samband med kreditupplysnings- och inkassoverksamhet behandlas uppgifter om enskildas personliga och ekonomiska förhållanden. Sådana uppgifter betraktas i allmänhet som integritetskänsliga. Behandlingen genomförs i stor utsträckning med hjälp av informationsteknik.

16.2 Kronofogdemyndigheten

16.2.1 Allmänt om Kronofogdemyndighetens behandling av personuppgifter

Kronofogdemyndigheten ansvarar för mål om betalningsföreläggande och handräckning, verkställighet och indrivning, skuldsanering samt tillsyn i konkurs m.m.

Mål om betalningsföreläggande och handräckning handlar i huvudsak om att en sökande försöker få en skuld, eller ett annat anspråk, fastställd i formell mening, dvs. genom ett särskilt beslut. Det kan exempelvis handla om att motparten ska åläggas att betala en skuld, återlämna viss egendom eller flytta från en lägenhet. Ett sådant beslut krävs i många fall för att sökanden ska kunna få hjälp med indrivning eller verkställighet av sitt anspråk. De uppgifter som Kronofogdemyndigheten behandlar i dessa mål inkluderar uppgifter om fysiska personers identitet, bostadsadresser och anställning, men även uppgifter om den aktuella tvisten och i vissa fall även tidigare tvister mellan parterna (vilket i vissa fall kan inkludera lagöverträdelser som innefattar brott, eller domar i brottmål). Behandlingen av uppgifter görs till stor del i en databas som benämns betalningsföreläggande- och handräckningsdatabasen. Uppgifter ur denna databas lämnas regelbundet ut till vissa kreditupplysningsföretag. Utlämnandet görs i viss utsträckning genom elektronisk överföring. Även parterna i målet kan i viss utsträckning erhålla uppgifter elektroniskt.

Mål och ärenden om verkställighet eller indrivning handlar i huvudsak om att en sökande vill ha hjälp att få betalt av motparten, eller att denne ska tvingas att göra något annat. Det kan t.ex. handla om att det ska göras en utmätning av lön, att viss egendom ska hämtas hos motparten eller säljas, eller att en hyresgäst ska vräkas. I dessa mål och ärenden behandlar Kronofogdemyndigheten bl.a. uppgifter om fysiska personers identitet, bostadsadresser, familje- och ekonomiska förhållanden samt uppgifter om den bakomliggande tvisten (vilket i vissa fall kan inkludera lagöverträdelser som innefattar brott, eller domar i brottmål). Denna behandling av uppgifter genomförs till stor del i en databas som benämns utsöknings- och indrivningsdatabasen. Uppgifter ur databasen överförs i viss utsträckning elektroniskt till Skatteverket och andra myndigheter, exempelvis till Försäkringskassan och länsstyrelserna. Elektronisk överföring görs i viss utsträckning även till vissa kreditupplysnings- och inkassoföretag samt – i mycket begränsad omfattning – till parterna i målet eller ärendet.

Ärenden om skuldsanering handlar i huvudsak om ifall en fysisk person, som är på obestånd och så skuldsatt att han eller hon inte kan antas ha förmåga att betala sina skulder inom överskådlig tid, helt eller delvis ska befrias från skyldigheten att betala sina skulder. I dessa ärenden behandlar Kronofogdemyndigheten bl.a. uppgifter

om fysiska personers identitet, bostadsadresser, familjeförhållanden och ekonomiska förhållanden, inklusive uppgifter om de aktuella skulderna (vilket i vissa fall kan inkludera lagöverträdelser som innefattar brott, eller domar i brottmål). Denna behandling av uppgifter utförs till stor del i en databas som benämns skuldsaneringsdatabasen.

I ärenden om tillsyn i konkurs, inklusive tillsyn över lönegaranti och företagsrekonstruktion med mera, behandlar Kronofogdemyndigheten uppgifter om fysiska personer, exempelvis konkursförvaltares och konkursbons identitet samt uppgifter om domstolsavgöranden och åtgärder i ärendena. Databasen får även tillföras vissa andra uppgifter, men det är inte så vanligt förekommande. Personuppgifter behandlas elektroniskt i en databas, som benämns konkurstillsynsdatabasen.

16.2.2 Det skyddande regelverket

Myndighetens behandling av personuppgifter regleras framför allt i lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet och i förordningen (2001:590) om behandling av uppgifter i Kronofogdemyndighetens verksamhet.

Lagen om behandling av uppgifter i Kronofogdemyndighetens verksamhet innehåller bl.a. bestämmelser om vilka uppgifter som myndigheten får ha i sina databaser och hur uppgifterna får hanteras där. Regleringen överensstämmer i vissa avseenden med motsvarande reglering i personuppgiftslagen (1998:204), men det finns även skillnader. En sådan skillnad är att Kronofogdemyndigheten enligt huvudregeln inte får lämna ut uppgifter till enskilda i digital form. I den mån sådana utlämnanden är tillåtna, exempelvis till godkända kreditupplysnings- och inkassoföretag samt andra myndigheter, krävs att utlämnandet görs på ett sätt som säkerställer att uppgifterna under översändandet inte blir förstörda eller förvanskade eller tillgängliga för andra än dem som de ska skickas till.

Av betydelse i detta sammanhang är även bestämmelserna i 2 kap. tryckfrihetsförordningen samt 34 kap. offentlighets- och sekretesslagen (2009:400). Offentlighetsprincipen innebär att Kronofogdemyndigheten är skyldig att lämna ut allmänna handlingar till den som begär det, om inte sekretess gäller för uppgifterna i handlingen. Hos myndigheten gäller sekretess för uppgifter om en enskilds

personliga eller ekonomiska förhållanden, men sekretessen varierar i styrka. Den är t.ex. starkare i ärenden om utsökning och indrivning än i ärenden om skuldsanering eller om tillsyn i konkurs. Det finns dessutom vissa undantag från sekretessen. Sekretess gäller t.ex. inte för uppgift om den förpliktelse som avses med den sökta verkställigheten i ett pågående mål och inte heller för beslutet i målet eller ärendet. Uppgift om en förpliktelse i ett avslutat mål omfattas inte heller av sekretess om den enskilde har ytterligare mål eller ärende registrerat hos Kronofogdemyndigheten och uppgiften inte är äldre än två år (den s.k. tvåårsregeln).

16.2.3 Tillstånd och tillsyn

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen och har i uppgift att värna skyddet för enskildas personliga integritet vid behandling av personuppgifter. Vidare utövar Riksdagens ombudsmän (Justitieombudsmannen) tillsyn över statliga myndigheter – däribland Kronofogdemyndigheten – och ska särskilt se till att grundläggande fri- och rättigheterna inte kränks i den offentliga verksamheten. Även Justitiekanslern (JK) utövar tillsyn över Kronofogdemyndigheten och har bl.a. i uppgift att värna integriteten samt rättssäkerheten i den offentliga verksamheten.

16.2.4 Risker för den personliga integriteten

Från att tidigare ha varit flera myndigheter, är Kronofogdemyndigheten numera en myndighet. En stor mängd uppgifter om enskildas personliga och ekonomiska förhållanden behandlas hos myndigheten inom ramen för dess olika verksamhetsgrenar. Myndigheten samlar bl.a. in en stor mängd uppgifter om gäldenärernas personliga förhållanden för att utreda om de har några utmätningsbara tillgångar. Denna kartläggning görs numera med stor precision. Även om alla uppgifter inte är speciellt känsliga om de bedöms var för sig, kan de sammantaget ge en helhetsbild av en enskild som kan upplevas som närgången och integritetskränkande.

Det är därför viktigt att myndigheten begränsar den interna åtkomsten till uppgifterna på lämpligt sätt. En grundläggande princip är att anställda inom en myndighet endast bör ha elektronisk tillgång till personuppgifter som de behöver för att utföra sitt arbete. Detta gäller även om uppgifterna är offentliga.

Datainspektionen förelade Kronofogdemyndigheten i ett beslut den 23 juni 2009[1] att komma in med en åtgärdsplan om hur myndigheten avser att utföra systematiska och återkommande logguppföljningar att upptäcka och beivra obehörig åtkomst av personuppgifter i Kronofogdemyndighetens verksamhetssystem. Av beslutet framgår att Datainspektionen gjorde bedömningen att myndighetens behörighetstilldelning i övrigt höll god kvalitet, avseende såväl tekniska aspekter som rutiner.

En annan viktig del i skyddet för den personliga integriteten är den sekretess som gäller hos myndigheten. För att arbetet ska kunna bedrivas på ett ändamålsenligt sätt behöver Kronofogdemyndigheten skaffa sig uppgifter från andra myndigheter som ger underlag för att bedöma en gäldenärs betalningsförmåga. Det kan röra sig om vitt skilda slag av uppgifter, som uppgifter från deklarationshandlingar eller uppgifter om anstaltsvistelser, arbetslöshet och sjukdomar. Uppgifter inhämtas i viss utsträckning även från gäldenären själv. Oavsett ursprung omfattas uppgifterna ofta av sekretess hos Kronofogdemyndigheten. Myndighetens beslut omfattas dock inte av sekretess. I bl.a. mål och ärenden om utsökning eller indrivning gäller inte heller sekretess för uppgift om den förpliktelse som ansökan gäller om målet eller ärendet fortfarande pågår eller – om det har avslutats – verkställighet för någon annan förpliktelse söks inom två år eller om verkställighet tidigare sökts och uppgiften inte är äldre än två år. Under år 2014 presenterades ett förslag att begränsa nyss nämnda undantag från sekretess för vissa avslutade ärenden (den så kallade tvåårsregeln).[2] Frågan bereds i Regeringskansliet.[3]

Av offentlighetsprincipen följer att var och en rätt har rätt att ta del av uppgifter i Kronofogdemyndighetens databaser som inte är sekretessbelagda. Utlämnande av sådana uppgifter görs enligt huvudregeln i pappersform eller muntligen. För utlämnande till kre-

[1] Dnr 1755-2008.

[2] *Tillförlitligare kreditupplysningar – ett förbättrat integritetsskydd vid offentligrättsliga krav*, Ds 2014:60 s. 84 f.

[3] Ju 2014/5532/L2.

ditupplysningsföretagen, som har stort behov av uppgifterna, har dock Kronofogdemyndigheten en elektronisk tjänst. Genom denna tjänst får kreditupplysningsföretag som har tillstånd för sin verksamhet daglig information om förändringar i utsöknings- och indrivningsdatabaserna samt om gäldenärernas totala skuldsaldo. Den information som kreditupplysningsföretagen får del av är bl.a. uppgifter om nya mål och uppgifter om upprättade utredningsrapporter. En utredningsrapport är en sammanställning som Kronofogdemyndighetens gör när myndigheten har utrett en ansökan om verkställighet och därefter kommit fram till att gäldenären inte har tillgångar som räcker för att betala hela skulden. Av utredningsrapporterna framgår registrerade åtgärder, bl.a. vilka register som kontrollerats, vilka förrättningar som vidtagits, om tillgångar har hittats eller inte och om dessa i så fall har något utmätningsbart värde. Med hänsyn till innehållet i databaserna är det givetvis viktigt att tillgången till uppgifterna är begränsad och inte missbrukas.

16.3 Kreditupplysning

16.3.1 Allmänt om kreditupplysning

Kreditgivare behöver underlag för att kunna bedöma om en person ska beviljas kredit. För att förenkla kreditgivningen finns kreditupplysningsföretag som förser kreditgivarna med kreditupplysningar, dvs. med uppgifter, omdömen och råd av betydelse för att kunna bedöma risken för framtida betalningsförsummelser och kreditförluster.

Kreditupplysningsföretagen samlar in uppgifter om enskilda personers ekonomiska och personliga förhållanden samt om företags ekonomiska förhållanden. Alla personer över 15 år finns registrerade hos de största kreditupplysningsföretagen. Uppgifterna hämtas huvudsakligen från myndigheter. Typiskt sett registreras identitetsuppgifter – t.ex. namn, personnummer och adress – som hämtas från Statens personadressregister (SPAR), samt uppgifter om inkomst och innehav av fastighet som hämtas från Skatteverkets skatteregister och fastighetstaxeringsregister. Vidare registreras uppgifter om betalningsanmärkningar, t.ex. utslag i mål om betalningsföreläggande, restförda skatter och avgifter eller misslyckade utmätnings-

försök. Dessa uppgifter hämtas från Kronofogdemyndigheten. För juridiska personer, näringsidkare och näringsanknutna personer hämtas även vissa uppgifter från aktiebolagsregistret och handels- och föreningsregistret hos Bolagsverket samt från det allmänna företagsregistret (Basun) hos Statistiska centralbyrån.

De upplysningar som kreditupplysningsföretagen i sin tur lämnar till kreditgivarna (kreditupplysningen) består främst av ekonomisk information, såsom uppgifter om sökandens inkomster, fastighetsinnehav och betalningsförsummelser. Även andra personliga uppgifter kan lämnas, t.ex. fakta som ålder eller civilstånd. Även omdömen och råd kan – som tidigare nämnts – lämnas som ledning för en ekonomisk bedömning.

Numera lämnas kreditupplysningarna huvudsakligen genom att kreditgivarna har en uppkoppling mot kreditupplysningsföretagets register/databas på internet. Kreditupplysningar kan också lämnas på annat sätt, t.ex. i tryckta skrifter, på cd-skivor eller på usb-minnen.

16.3.2 Det skyddande regelverket

Kreditupplysningsverksamhet regleras i första hand i kreditupplysningslagen (1973:1173). Den lagen är enligt huvudregeln tillämplig dels när någon lämnar kreditupplysningar mot ersättning eller som ett led i näringsverksamhet, dels vid annan kreditupplysningsverksamhet som är av större omfattning.

Lagen syftar i första hand till att skydda de registrerades personliga integritet, men är även avsedd att bidra till en effektivt fungerande kreditupplysningsverksamhet. Den innehåller bl.a. ett generellt krav på att kreditupplysningsverksamhet ska bedrivas så att den inte leder till otillbörligt intrång i den personliga integriteten genom innehållet i de upplysningar som förmedlas eller på annat sätt.

Uppgifter om privatpersoner får enligt lagen bara lämnas ut om det finns legitimt behov. Det kan t.ex. vara nödvändigt med en kreditprövning när ett kreditavtal ska ingås eller i andra situationer då en ekonomisk riskbedömning behöver göras, t.ex. i borgens-, anställnings- eller hyressammanhang.[4]

[4] Regeringens proposition *Ett starkare skydd för den enskildes integritet vid kreditupplysning*, prop. 1973:155 s. 148.

För att säkerställa att upplysningar från kreditupplysningsregister är aktuella innehåller lagen bestämmelser om när uppgifter inte längre får användas och ska tas bort, dvs. gallras. Som exempel kan nämnas att uppgifter om privatpersoners betalningsanmärkningar ska gallras senast tre år efter den dag då anmärkningen tillkom och uppgifter om skuldsanering efter fem år.

När en kreditupplysning om en fysisk person lämnas ut ska personen få ett skriftligt meddelande om detta – i regel en kopia av upplysningen – för att kunna kontrollera att informationen som lämnats är korrekt.

Om en uppgift i ett register visar sig vara oriktig eller missvisande eller har behandlats i strid med kreditupplysningslagen, ska kreditupplysningsföretaget som huvudregel sända en rättelse eller komplettering till var och en som under den senaste tolvmånadersperioden fått del av uppgiften.

I kreditupplysningslagen finns även bestämmelser om straff för brott mot vissa av lagens bestämmelser, bl.a. i fråga om utlämnande av kreditupplysning utan att det finns ett legitimt behov eller om någon bedriver kreditupplysningsverksamhet utan att ha rätt till det. Vidare kan ett kreditupplysningsföretag under vissa förutsättningar bli skadeståndsskyldigt för skador som det tillfogar någon i sin verksamhet genom otillbörligt intrång i den skadelidandes personliga integritet eller genom att oriktig uppgift lämnas om personen.

Enligt kreditupplysningslagen gäller tystnadsplikt för den som är eller har varit verksam i kreditupplysningsverksamhet avseende uppgifter om enskildas personliga förhållanden eller om yrkes- eller affärshemlighet.

Personuppgiftslagen ska inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen (7 § personuppgiftslagen). Enligt 1 kap. 9 § yttrandefrihetsgrundlagen ska grundlagens regler om radioprogram även tillämpas på sådana databaser som tillhandahålls av s.k. massmedieföretag och på sådana databaser för vilka utgivningsbevis gäller. Utgivningsbeviset innebär således att databasen omfattas av det särskilda skydd för yttrandefriheten som anges i yttrandefrihetsgrundslagen. Enligt censurförbudet i 1 kap. 3 § yttrandefrihetsgrundlagen är det inte tillåtet för myndigheter och andra allmänna organ att utan stöd i yttrandefrihetsgrund-

lagen, på grund av det kända eller väntade innehållet i ett radioprogram eller en teknisk upptagning, förbjuda eller hindra dess offentliggörande eller spridning bland allmänheten.

Under vissa förutsättningar blir kreditupplysningslagens skyddsregler inte tillämpliga när kreditupplysningar lämnas ut på en teknisk upptagning. Regler om utlämnandet finns i såväl yttrandefrihetsgrundlagen som kreditupplysningslagen. Med *teknisk upptagning* avses upptagningar som innehåller text, bild eller ljud och som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Exempel på sådana tekniska upptagningar är usb-minne, cd- och dvd-skiva. Innebörden av dessa undantag i kreditupplysningslagen är att kravet på att det ska finnas ett legitimt behov av kreditupplysningen hos beställaren faller bort. Vidare gäller inte heller kravet på kreditupplysningskopia. Undantag gäller också för skyldigheten att sända en rättelse eller komplettering till var och en som har mottagit en upplysning med en oriktig eller missvisande uppgift eller en uppgift som har behandlats i strid med lagen. Även det åtföljande straffansvaret bortfaller.

Regleringen i kreditupplysningslagen kompletteras av vissa generella krav i personuppgiftslagen, bl.a. skyldigheten att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Personuppgiftslagens bestämmelser gäller alltså även vid kreditupplysning, om frågan inte är särskilt reglerad i exempelvis kreditupplysningslagen. Se närmare om personuppgiftslagen i kapitel 6 *Den grundläggande rättsliga regleringen*.

16.3.3 Tillstånd och tillsyn

För att bedriva kreditupplysningsverksamhet krävs normalt tillstånd från Datainspektionen. Det krävs även medgivande från Datainspektionen för att få överlåta eller upplåta register som används i kreditupplysningsverksamhet. Datainspektionen utövar dessutom tillsyn över att kreditupplysningslagen och personuppgiftslagen följs.

16.3.4 Risker för den personliga integriteten

Inledning

Uppgifter som ingår i kreditupplysningar är ofta av känslig karaktär och kan utnyttjas till men för den enskilde. Samtidigt är det en förutsättning för en fungerande kreditmarknad att kreditgivare har tillgång till ett bra underlag som gör det möjligt att bedöma risken för kreditförluster. I detta ligger också att kreditupplysningen måste fungera effektivt.

Kreditupplysningsföretagens insamling och lagring av uppgifter

Det finns en risk att kreditupplysningsföretag samlar in, eller önskar samla in, uppgifter vars relevans för kreditbedömningen kan ifrågasättas. Det förekommer t.ex. att kreditupplysningsföretag önskar samla in uppgifter om antalet mobilabonnemang som en person fått beviljat. Sådana uppgifter har i praxis inte ansetts uppfylla de krav på adekvans, relevans och proportionalitet som gäller för insamling av personuppgifter.[5]

Det finns också en risk att de uppgifter som behandlas inte är korrekta och aktuella. Det är därför viktigt att kreditupplysningsföretagen uppfyller sin skyldighet att utreda om en uppgift som behandlas eller lämnats i kreditupplysning är oriktig eller missvisande, om det finns anledning att misstänka att så är fallet. Det är även viktigt att uppgifter i register som visar sig vara oriktiga eller missvisande rättas, kompletteras eller utesluts ur registret. Om ett företag inte rättar uppgifterna frivilligt kan det föreläggas att göra detta. I praxis har det bl.a. förekommit att ett kreditupplysningsföretag har förelagts att ta bort en uppgift om en ansökan om konkurs, på grund av att den aktuella ansökan inte ansågs ha varit allvarligt menad och därför var missvisande i kreditupplysningslagens mening.[6]

Registren omfattar ofta en väsentlig del av Sveriges befolkning, vilket i sig innebär särskilda risker. Det är dessutom fråga om en sammanställning och kartläggning av enskilda personer, vilket är att betrakta som känslig information. Kreditupplysningsverksamhet omgärdas av tystnadsplikt och det är inte tänkt att andra än den som

[5] Kammarrättens i Stockholm dom den 20 november 2014 i mål nr 3148-14.
[6] Förvaltningsrättens i Stockholm dom den 21 juli 2015 i mål nr 3013-15.

har ett legitimt behov ska kunna ta del av uppgifterna. Om någon skaffar sig obehörig åtkomst till registret är många människor exponerade för att deras uppgifter sprids. Det är därför viktigt att uppgifterna skyddas på ett betryggande sätt. Datainspektionen har i olika sammanhang betonat att det ställs höga krav på säkerhet när det gäller denna typ av uppgifter, se bl.a. nedan angående stark autentisering.

Kreditupplysningsföretagens utlämnande av uppgifter

De uppgifter om enskildas personliga och ekonomiska förhållanden som kreditupplysningsföretagen hanterar är ofta av känslig natur. Det gäller särskilt när uppgifterna sammanställs och lagras på det sätt som ofta görs i kreditupplysningsföretagens databaser. Oönskad spridning av uppgifterna kan därför få stora negativa konsekvenser för enskildas personliga integritet.

Med undantag för vissa offentliggöranden enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen, får kreditupplysningar om fysiska personer, som inte är näringsidkare inte lämnas ut om det finns anledning att anta att upplysningen kommer att användas av någon annan än den som på grund av ett ingånget eller ifrågasatt kreditavtal eller av någon liknande anledning har behov av upplysningen. För att säkerställa att detta förbud följs är det är av stor vikt att kreditupplysningsföretagen alltid kontrollerar att beställaren av uppgifter har ett sådant legitimt behov av uppgifterna.

Det finns exempel på att kreditupplysningsföretag har lämnat ut ett stort antal kreditupplysningar utan att vare sig vid ingående av kundavtalet eller i samband med själva utlämnandet ha kontrollerat om mottagaren kan antas ha ett legitimt behov av personupplysningar. Ett sådant utlämnande anses strida mot nämnda förbud. Ett kreditupplysningsföretag kan alltså inte uppfylla kravet på kontroll genom att exempelvis endast ta in bestämmelser i sina avtal som anger dels att kunden endast får beställa uppgifter när denne har ett legitimt behov av dem, dels att det är kundens ansvar att se till att detta krav är uppfyllt.[7]

Det har till och med inträffat att kreditupplysningar har lämnats ut utan att kreditupplysningsföretaget alls har beaktat kravet på legitimt behov, på grund av att företaget har trott att det kravet inte

[7] Datainspektionens beslut den 12 maj 2014, dnr 183-2014.

gäller för dess verksamhet.[8] Det går inte att undgå kreditupplysningslagens skyddsregler genom att exempelvis lämna ut uppgifter om hur en enskild persons inkomst förhåller sig till andra personers inkomster, i stället för att ange inkomsten i exakta tal.[9] Det finns dock företag som begränsar den information som lämnas ut på andra sätt, för att undvika en tillämpning av skyddsreglerna. Om ett sådant företag har ett utgivningsbevis gäller inte heller personuppgiftslagens skyddsregler. Personuppgiftslagen gäller inte då personuppgifter publiceras på webbplatser som omfattas av yttrandefrihetsgrundlagen.

Om utlämnandet av kreditupplysningar görs via internet finns dessutom en risk att obehöriga får tillgång till uppgifter och att uppgifterna därefter får stor spridning på internet. Ett utlämnande av känsliga uppgifter via öppet nät, exempelvis internet, får därför endast göras om mottagarens identitet är säkerställd med stark autentisering, t.ex. e-legitimation eller vissa lösningar med engångslösenord eller motsvarande. För att uppfylla kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen anses det alltså inte vara tillräckligt att använda autentisering med enbart användarnamn och lösenord.[10]

En annan viktig del i integritetsskyddet är kravet att en kreditupplysningskopia ska lämnas till den som upplysningarna avser. Kopian ger den enskilde en möjlighet att kontrollera att de uppgifter som lämnas är korrekta och fullständiga, och att bl.a. kravet på legitimt behov följs. Lämnandet av en kopia kan också vara ett sätt att upptäcka missbruk av inloggning till en databas. Brister när det gäller distributionen av kopior kan därför få stora konsekvenser för den personliga integriteten. I praxis har konstaterats att det i och för sig kan vara tillräckligt att distribuera kopian digitalt, men att kopian ska sändas till en plats som är, eller kan jämställas med, den omfrågades adress. Det är alltså inte tillräckligt att utan föregående överenskommelse skicka en länk till en webbsida där den omfrågade kan hitta den aktuella informationen.[11] Det är inte heller tillräckligt att förse den

[8] Förvaltningsrättens i Stockholm dom den 1 november 2012 i mål nr 14578-11.
[9] Datainspektionens beslut den 18 september 2013, dnr 833-2103 och 834-2013.
[10] Kammarrättens i Stockholm dom den 31 januari 2014 i mål nr 8237-12.
[11] Förvaltningsrättens i Stockholm dom den 14 maj 2014 i mål nr 22551-11.

omfrågade med all information som finns hos kreditupplysningsföretaget, utan det ska av kopian framgå vilka av dessa uppgifter som har lämnats ut.[12]

Avslutningsvis ska nämnas att det även ställs krav på den som ta emot kreditupplysningen. Kreditgivaren får t.ex. inte använda alltför gamla uppgifter vid kreditprövningen, eftersom de efter viss tid inte längre anses vara adekvata och relevanta. Hänsynen till den enskilde kräver bl.a. att denne inte för all framtid belastas med en uppgift om t.ex. enstaka betalningsförsummelser. Det är med andra ord inte tillräckligt att uppgifterna var aktuella när kreditgivaren erhöll kreditupplysningen.[13] Se vidare kapitel 15 om bank- och kreditmarknaden.

Särskilt om utgivna tekniska upptagningar

Många av de integritetsskyddande reglerna, bl.a. bestämmelserna om legitimt behov, lämnande av kreditupplysningskopia och skyldigheten att sända en rättelse eller komplettering till var och en som har mottagit en upplysning med en oriktig eller missvisande uppgift eller en uppgift som har behandlats i strid mot lagen, gäller i dagsläget inte för utlämnande av kredituppgifter med hjälp av tekniska upptagningar, t.ex. usb-minnen, som är utgivna med stöd av yttrandefrihetsgrundlagen. Under senare tid har det uppstått nya former av kreditupplysningstjänster via utgivna tekniska upptagningar. Även sådana utlämnanden kan för närvarande göras med stöd av yttrandefrihetsgrundlagen, utan hänsyn till de integritetsskyddande bestämmelserna i kreditupplysningslagen. Exempelvis ett usb-minne kan innehålla en stor mängd information om många personer, som dessutom kan göras sökbar. Även sådana utlämnanden innebär alltså en stor risk för enskildas personliga integritet.

Efter en inspektion av samtliga Sveriges större kreditupplysningsföretag konstaterade Datainspektionen i en hemställan till regeringskansliet, att syftet med lagstiftningen inte hade uppnåtts, eftersom det uppstått nya möjligheter för en abonnent att på ett lättillgängligt sätt ta del av kreditupplysningar utan hänsyn till nämnda regelverk.[14]

[12] Datainspektionens beslut den 1 november 2011, dnr 1826-2010.
[13] Datainspektionens beslut den 9 juni 2014, dnr 1823-2013 och 1826-2013.
[14] Datainspektionens hemställan den 6 mars 2012, dnr 1821-2010.

Att kreditupplysningar kan lämnas ut trots att beställaren av upplysningen saknar legitimt behov innebär att vem som helst kan få reda på uppgifter, som inte sällan är känsliga, om enskilda personer i Sverige. Den person som uppgifterna avser saknar därmed möjlighet att styra över vem som får ta del av kreditupplysningar om honom eller henne. Det är ett betydande intrång i den personliga integriteten. Att det i dessa fall inte heller skickas någon kreditupplysningskopia innebär ytterligare integritetsrisker, liksom att andra integritetsskyddande bestämmelser inte är tillämpliga.

Det är av nämnda skäl mycket angeläget att en teknikoberoende lagstiftning kommer till stånd. Kommittén konstaterar dock att det redan har presenterats ett förslag till sådan lagstiftning, som för närvarande bereds i regeringskansliet.[15] Kommittén har därför valt att inte fördjupa sig ytterligare i den frågan.

16.4 Inkasso

16.4.1 Allmänt om inkassoverksamhet

Den som inte betalar sina skulder kan bli föremål för inkassoåtgärder. Med inkassoåtgärd menas en påtryckning på gäldenären, till exempel ett inkassokrav eller en ansökan om betalningsföreläggande. Det är däremot inte en inkassoåtgärd att på en faktura eller en betalningspåminnelse ange tid för betalning eller att fordran kommer att överlämnas för inkasso om den inte betalas.

Inkassoverksamhet kan bedrivas som egeninkasso, dvs. när en fordringsägare som själv bedriver näringsverksamhet driver in fordringar som uppkommit i den egna verksamheten. Indrivningen kan också utföras genom ombud som bedriver inkassoverksamhet.

Uppgifter som förekommer i inkassoverksamhet är normalt att anse som känsliga.

[15] *Ett teknikoberoende skydd för den enskildes integritet vid kreditupplysning*, Ds 2013:27, beredning pågår inom regeringskansliet (dnr Ju/2013/3527/L2).

16.4.2 Det skyddande regelverket

Inkassoverksamhet regleras främst i inkassolagen (1974:182). Lagen syftar i första hand till att skydda gäldenärer mot otillbörliga inkassometoder, som trakasserier och onödiga kostnader. Lagen innehåller också. vissa bestämmelser om register i inkassoverksamhet och om förbud mot obehörigt röjande eller utnyttjande av uppgifter om personliga förhållanden, som man fått del av inom ramen för inkassoverksamhet. Den innehåller däremot inte några andra bestämmelser som rör behandling av personuppgifter. För den personuppgiftsbehandling som utförs inom ramen för inkassoverksamhet gäller därför personuppgiftslagens regler (se kapitel 6 *Den grundläggande rättsliga regleringen*).

16.4.3 Tillstånd och tillsyn

För att få bedriva inkassoverksamhet som ombud krävs Datainspektionens tillstånd, om verksamheten inte bedrivs av företag som står under Finansinspektionens tillsyn eller av advokater.

Datainspektionen har tillsyn över att inkassolagens bestämmelser följs och att inkassoverksamhet bedrivs enligt god inkassosed, dvs. att gäldenären inte vållas onödig skada eller olägenhet eller utsätts för otillbörlig påtryckning eller annan otillbörlig inkassoåtgärd. Datainspektionen har också tillsynsansvar för att personuppgifter behandlas på ett sätt som är förenligt med personuppgiftslagen.

16.4.4 Risker för den personliga integriteten

Eftersom inkassobolag behandlar uppgifter som är känsliga från integritetssynpunkt, är det bl.a. viktigt att behandlingen inte avser fler uppgifter än vad som behövs, att gallring görs på ett korrekt sätt och att oönskad spridning av uppgifterna undviks.

De problem som hittills uppmärksammats har främst gällt risken för oönskad spridning av uppgifterna.

Under våren 2010 genomförde Datainspektionen ett projekt som benämndes *Gäldenärswebbar*. Inom ramen för detta projekt granskade Datainspektionen sex inkassobolags webbtjänster. Syftet var att undersöka för vilka ändamål gäldenärswebbarna användes, hur

systemen var utformade, vilka personuppgifter om gäldenären som behandlades, hur skyddade personuppgifter hanterades och om inkassobolagen vidtog lämpliga säkerhetsåtgärder för att skydda de personuppgifter som behandlades. Vid denna granskning konstaterade Datainspektionen sammanfattningsvis att den behandling som ägde rum i och för sig var tillåten, men att det var alltför enkelt för utomstående att bereda sig tillgång till informationen på webbtjänsterna. Inloggning kunde i regel genomföras med enkla användarnamn och lösenord, vilka i vissa fall till och med bestod av kombinationer som ärendenummer och person- eller OCR-nummer. Datainspektionen förelade därför inkassobolagen att i webbtjänsterna säkerställa gäldenärernas identitet genom en teknisk funktion som ger en stark autentisering, t.ex. e-legitimation. Sedan vissa av inkassobolagen överklagat dessa beslut har Kammarrätten i Stockholm bekräftat att det, för att uppfylla personuppgiftslagens säkerhetskrav, krävs stark autentisering i dessa fall.[16]

Det har även inträffat att inkassobolag har skickat brev, med uppgift om bl.a. namn, adress och skuld, till fel person. Ett uppmärksammat exempel på detta är att ett inkassobolag under sommaren 2015 skickade drygt 7 000 sådana brev till fel personer.[17] Inkassobolaget har dock uppmärksammat Datainspektionen på felet och en utredning av det inträffade pågår fortfarande. Riskerna för sådana misstag torde öka om verksamheten effektiviseras ytterligare, exempelvis om vissa aktörer skulle överväga att börja distribuera inkassokrav via e-post.

16.5 Kommitténs samlade bedömning av området

I detta kapitel har kommittén analyserat integritetsrisker i samband med Kronofogdemyndighetens, kreditupplysningsföretagens och inkassobolagens verksamhet.

Kronofogdemyndigheten behandlar en stor mängd uppgifter om många enskildas personliga och ekonomiska förhållanden. Det är därför nödvändigt att den interna åtkomsten till uppgifterna begrän-

[16] Kammarrättens i Stockholm domar den 6 mars 2013, mål nr 2415-12, 2416-12, 2417-12, 2418-12 och 2419-12.

[17] Metro, *Tusentals svenskar fick inkassobrev av misstag*, publicerad den 3 september 2015 på www.metro.se

sas på lämpligt sätt. Myndigheten lämnar dagligen ut information om förändringar i utsöknings- och indrivningsdatabaserna samt om gäldenärernas totala skuldsaldo i elektronisk form till kreditupplysningsföretagen. Uppgifterna måste skyddas från en större spridning än vad som är motiverad samt att inte vilka aktörer som helst får tillgång till uppgifterna i digital form. Kronofogdemyndigheten behandlar känsliga uppgifter om gäldenärer, men behandlar inte uppgifter om hela befolkningen. Kommittén har inte fått information om stora brister i myndighetens hantering av personuppgifter. Mot den bakgrunden bedömer kommittén att det finns vissa risker den personliga integriteten i kronofogdemyndighetens verksamhet.

Kreditupplysningsföretagens verksamhet bygger på att de samlar in stora mängder känsliga uppgifter om hela befolkningen som på olika sätt kan ha betydelse vid kreditgivning. Det ligger i sakens natur att det finns en risk att de samlar in fler uppgifter än vad som verkligen är motiverat. Det finns också en risk att vissa insamlade uppgifter inte är korrekta och aktuella samt för att de lagras längre än nödvändigt.

Den enskilde har i vart fall i teorin vissa möjligheter att påverka kreditupplysningsföretagens utlämnande av uppgifter, genom att undvika lån och krediter, men saknar i princip möjlighet att påverka vilka uppgifter som samlas in.

För att minimera riskerna med kreditupplysningsföretagens verksamhet innehåller lagstiftningen olika typer av integritetsskyddande regler. Ett exempel på detta är kravet på att uppgifter som är oriktiga eller missvisande ska rättas, kompletteras eller uteslutas ur registret. Ett annat exempel är kravet på att obehörig tillgång till registren ska motverkas. I detta ligger bl.a. att företagen måste kontrollera att mottagaren har ett legitimt behov av uppgifterna och att utlämnandet görs på ett säkert sätt. Även kravet på att en kreditupplysningskopia ska lämnas till den som upplysningarna avser är viktigt för att minimera risken för integritetsintrång. Tack vare denna kopia får den enskilde bl.a. en möjlighet att kontrollera att de uppgifter som lämnas är korrekta och fullständiga, och att bl.a. kravet på legitimt behov följs.

För närvarande gäller de integritetsskyddande bestämmelserna i kreditupplysningslagen inte vid vissa former av offentliggörande enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Det gäller t.ex. utlämnanden av uppgifter på tekniska upptagningar, t.ex.

på usb-minnen. Sådana utlämnanden innebär en avsevärd risk från integritetssynpunkt. Det är angeläget att de integritetsskyddande bestämmelserna görs tillämpliga även på sådana utlämnanden. Mot bakgrund av de ovannämnda riskerna i samband med hantering av känsliga uppgifter om hela befolkningen bedömer kommittén att det föreligger allvarliga risker den personliga integriteten i kreditupplysningsföretagens verksamhet. Kommittén noterar dock att frågan har utretts och för närvarande bereds i regeringskanslitet.

Även *inkassobolag* behandlar stora mängder uppgifter som är känsliga från integritetssynpunkt. De behandlar dock inte uppgifter om lika många personer som kreditupplysningsföretagen. Det finns dock också i sådan verksamhet en risk att behandlingen avser fler uppgifter än nödvändigt, att vissa uppgifter är felaktiga eller inaktuella och, framför allt, att uppgifterna sprids på ett oönskat sätt. I det sistnämnda ligger bl.a. att det måste säkerställas att uppgifterna inte skickas till, eller är åtkomliga för, utomstående. I denna verksamhet är därför personuppgiftslagens krav på säkerhetsåtgärder – och Datainspektionens tillsynsverksamhet – av särskild betydelse.

Kommittén bedömer att det föreligger vissa risker för intrång i den enskildes integritet på grund av behandling av personuppgifter i inkassobolagens verksamhet.

17 Domstolarnas verksamhet

Kommitténs bedömning: Det finns en viss risk för den personliga integriteten i samband med personuppgiftsbehandling i domstolarnas verksamhetsregister, i samband med ljud- och bildupptagningar och i samband med informationsutbyte med andra myndigheter.

Det föreligger påtagliga risker för den personliga integriteten i samband med utlämnande av uppgifter på medium för automatiserad behandling.

17.1 Inledning

17.1.1 Om domstolarna

De allmänna domstolarna utgörs av tingsrätterna, hovrätterna och Högsta domstolen. Förvaltningsdomstolarna består av länsrätterna, kammarrätterna och Högsta förvaltningsdomstolen. Därtill finns ett antal specialdomstolar, bl.a. Marknadsdomstolen och Arbetsdomstolen.

I de allmänna domstolarna handläggs framför allt brottmål och tvistemål. Därutöver handlägger de allmänna domstolarna diverse ärenden, t.ex. rörande godmanskap, förvaltarskap och tillstånd till adoption.

I förvaltningsdomstolarna handläggs framför allt olika typer av tvister mellan den enskilde och det allmänna i form av kommun, landsting eller stat. Vid förvaltningsdomstolarna handläggs t.ex. socialförsäkringsmål, skattemål, migrationsmål samt beslut om tvångsingripanden för ungdoms-, missbruks- eller psykiatrivård.

Verksamheten i domstolarna är av sådan karaktär att det förekommer uppgifter om enskildas personliga förhållanden i mycket stor utsträckning. Uppgifterna är dessutom många gånger av känslig natur. I vissa fall är det den enskilde själv som lämnar sina personuppgifter till domstolen, t.ex. vid väckande av talan. I andra fall lämnas uppgifterna av en motpart, vilket inte sällan är en myndighet, eller av någon annan aktör som lämnar uppgifter till domstol, t.ex. Kriminalvården. Även personuppgifter om andra än parterna behandlas i stor utsträckning, bl.a. namn och adressuppgifter för vittnen som åberopas i processerna, men också närmare uppgifter om t.ex. anhörigas personliga förhållanden i mål och ärenden där familjeförhållanden är av betydelse.

Av rättssäkerhetsskäl är det av stor vikt att domstolarnas verksamhet utövas under öppenhet. Möjligheten till insyn är också en förutsättning för allmänhetens förtroende för domstolarna. En utgångspunkt är därför att så mycket som möjligt ska vara offentligt. I domstolarnas verksamhet finns således en motsättning mellan den enskildes intresse av skydd för den personliga integriteten samt intresset av en rättssäker men även effektiv process.

I detta kapitel behandlas domstolarnas användning av informationsteknik i den rättsskipande och rättsvårdande verksamheten.

17.1.2 Domstolarnas användning av informationsteknik

Modern informationsteknik är en naturlig del i domstolarnas arbete och den elektroniska ärendehanteringen har ökat. I princip all framställning av skriftlig information hos domstolarna görs på elektronisk väg, och domstolarna tar i allt större utsträckning emot och lagrar information i elektronisk form. Diarieföring i mål och ärenden görs i det elektroniska verksamhetsstödet Vera. I Vera görs också ljud- och bildupptagning av framför allt förhör som hålls vid förhandling i domstol. Vidare används e-post i allt större utsträckning för domstolarnas kommunikation med bl.a. parter och ombud. Domstolarna får ta emot handlingar, t.ex. yttranden från parter, per e-post och använder också e-post för att bl.a. expediera handlingar såsom domar och beslut till inblandade aktörer. Även utlämnande av

allmänna handlingar görs till viss del per e-post. Uppgifter överförs även elektroniskt mellan olika tekniska system hos domstolarna och vissa andra myndigheter inom rättsväsendet.

17.1.3 Den rättsliga regleringen

Offentlighet och sekretess vid domstol

En grundläggande princip i det svenska statsskicket är offentlighetsprincipen. Principen innebär att var och en har stora möjligheter till insyn i myndigheternas arbete. Reglerna om allmänhetens rätt att ta del av allmänna handlingar återfinns i 2 kap. tryckfrihetsförordningen samt offentlighets- och sekretesslagen (2009:400). En domstol är skyldig att lämna ut allmänna handlingar, om inte sekretess gäller för uppgifterna i handlingen. Sekretess innebär ett förbud att röja uppgifter och vilka uppgifter som omfattas av sekretess följer av offentlighets- och sekretesslagen. I domstol gäller sekretess för olika slags uppgifter, t.ex. när det gäller sexualbrottsmål, personalia i brottmål, familjemål, affärs- och driftförhållanden, offentlig upphandling samt ärenden som rör socialförsäkring. Under vissa förutsättningar kan också sekretess för uppgifter överföras till och från en annan myndighet. Sekretess hindrar i princip inte att en part i ett mål eller ärende tar del av handling eller annat material i målet eller ärendet.

Det finns ett starkt intresse av insyn i domstolarnas verksamhet, vilket i många fall leder till att uppgifter som i andra sammanhang är skyddade genom sekretess blir tillgängliga för utomstående.

I promemorian *Offentlighet och sekretess för uppgifter i domstolsavgöranden*[1] föreslås vissa ändringar av de bestämmelser som reglerar offentlighet och sekretess för uppgifter som tas in i vissa avgöranden hos domstolarna. Det föreslås bl.a. att en domstol ska kunna besluta om fortsatt sekretess för uppgift i domslut eller motsvarande del i ett beslut, om domstolen gör bedömningen att intresset av sekretess för uppgiften väger väsentligt tyngre än intresset av offentlighet. Det handlar framför allt om möjligheten att med hänsyn till den personliga integriteten hemlighålla identiteten på t.ex. en part.

[1] Ds 2014:33.

En ny domstolsdatalag

Domstolsdatalagen (2015:728) trädde i kraft den 1 januari 2016 och ersätter förordningarna om registerföring m.m. vid domstolarna och nämnderna. Som skäl för förslaget till en ny lag angavs i propositionen[2] bl.a. att en stor omfattning av personuppgiftsbehandlingen i domstolarna medför ett sådant intrång i enskildas personliga integritet som avses i 2 kap. 6 § regeringsformen, vilket innebär att behandlingarna endast kan tillåtas genom bestämmelser i lag (jfr 2 kap. 20 § första stycket 2 RF). Lagen innehåller ramarna för domstolarnas personuppgiftsbehandling samt de bestämmelser som är av central betydelse för integritetsskyddet. Enligt propositionen bör kompletterande bestämmelser meddelas genom förordning. De föreskrifter regeringen meddelar får dock inte innebära ett betydande intrång i den personliga integriteten (jfr 2 kap. 6 § andra stycket RF).[3]

Enligt domstolsdatalagen får personuppgifter behandlas om det behövs för handläggning av mål och ärenden eller för författningsenligt uppgiftslämnande. Vidare ska tillgången till personuppgifter begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter. Personuppgifter får lämnas ut på medium för automatiserad behandling om det inte är olämpligt. Med utlämnande på medium för automatiserad behandling avses bl.a. utlämnande på ett usb-minne, genom e-post, eller annan elektronisk överföring. Lämplighetsprövningen ska göras i varje enskilt fall. Det har vid lämplighetsprövningen betydelse vem mottagaren är. I fråga om utlämnande till en annan domstol eller en myndighet bör enligt förarbetena[4] utlämnande på medium för automatiserad behandling som utgångspunkt vara tillåtet enligt bestämmelsen. I fråga om utlämnande av processmaterial till en part eller partens ombud, biträde eller försvarare måste kravet på en rättvis rättegång och andra processrättsliga principer beaktas. Exempelvis bör en part som regel få ta del av processmaterialet i elektronisk form om det behövs för att säkerställa att parterna i en process är likställda.

[2] Regeringens proposition *Domstolsdatalag*, prop. 2014/15:148.
[3] Prop. 2014/15:148 s. 22 f.
[4] Prop. 2014/15:148 75 f. och 113 f.

17.1.4 Tillsyn

Riksdagens ombudsmän, Justitieombudsmannen, utövar tillsyn bl.a. över statliga myndigheter – däribland domstolarna – och ska särskilt utöva tillsyn över att grundläggande fri- och rättigheterna inte kränks i den offentliga verksamheten.

Även Justitiekanslern utövar tillsyn över domstolarna och har bl.a. i uppgift att värna integriteten samt rättssäkerheten i den offentliga verksamheten.

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen och har i uppgift att värna skyddet för enskildas personliga integritet vid behandling av personuppgifter.

17.2 Behandling av uppgifter i verksamhetsregister och besöksterminaler

17.2.1 Företeelsen

Diarieföringen i den rättsskipande och rättsvårdande verksamheten görs i det elektroniska verksamhetsstödet Vera. Där registreras olika sorters uppgifter som rör handläggningen av mål och ärenden, såsom måluppgifter (bl.a. målnummer och saken), partsuppgifter (t.ex. namn, personnummer och adress), uppgifter om vittnen och ombud m.fl. samt uppgifter om domstolens handläggningsåtgärder och beslut. Varje domstol har ett eget verksamhetsregister i Vera, men uppgifterna lagras hos Domstolsverket.

17.2.2 Det skyddande regelverket

Den 1 januari 2016 trädde domstolsdatalagen i kraft. Lagen ersätter bl.a. de förordningar (Vera-förordningarna) som tidigare reglerade olika domstolars behandling av personuppgifter. Enligt denna lag får domstolarna behandla personuppgifter om det behövs för handläggning av mål och ärenden.

Domstolsdatalagen hänvisar till personuppgiftslagens bestämmelser om grundläggande krav för personuppgiftsbehandling. Det innebär bl.a. att

- de behandlingar som utförs måste vara lagliga och göras på ett korrekt sätt och i enlighet med god sed,
- personuppgifterna som behandlas måste vara nödvändiga, adekvata, relevanta och riktiga,
- personuppgifter får samlas in endast för särskilda och uttryckligt angivna ändamål, och
- insamlade personuppgifter inte får vidarebehandlas för ett ändamål som är oförenligt med det ändamål som uppgifterna samlades in för.

Enligt domstolsdatalagen är det vidare förbjudet att som sökbegrepp använda uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, sexualliv, nationell anknytning, eller brott eller misstanke om brott. Förbudet gäller dock inte användning av uppgifter som avslöjar brott eller misstanke om brott i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamheter samt användning av uppgifter som avslöjar hälsa i de allmänna förvaltningsdomstolarnas verksamhet.[5]

17.2.3 Risker för den personliga integriteten

Ett automatiskt register som Vera kan vara mycket effektivt och gör det bl.a. enkelt att anteckna olika händelser i diariet. Registret kan också användas för att via s.k. besöksterminaler ge allmänheten tillgång till uppgifter som de har rätt att ta del av. Det är dock viktigt att diariet inte innehåller personuppgifter som inte får behandlas på sådant sätt.

Justitiekanslern har vid inspektion vid en tingsrätt noterat i ett flertal akter att tingsrättens dagboksblad innehöll anteckningar om känsliga personuppgifter avseende enskildas hälsotillstånd, vilket inte varit förenligt med regleringen i 13 § personuppgiftslagen.[6]

[5] Prop. 2014/15:148 s. 57 f.
[6] Justitiekanslerns beslut den 20 januari 2014, dnr 7004-13-28.

Vidare har Datainspektionen i fyra beslut[7] efter inspektion hos tre tingsrätter och en förvaltningsrätt, riktat kritik mot att det i domstolarnas besöksterminaler var möjligt att kartlägga hur enskilda personer förekommer i olika mål och ärenden. I besluten framhåller Datainspektionen bl.a. att besöksterminalerna innehåller fler och känsligare uppgifter än ett diarium måste innehålla samt gör det möjligt att genomföra sökningar baserat på namn och personnummer. Denna behandling går enligt Datainspektionen utöver vad som är nödvändigt för att tillgodose kraven enligt offentlighetsprincipen och strider därför mot personuppgiftslagen. Datainspektionen förelade domstolarna att i besöksterminalerna endast behandla de uppgifter som är nödvändiga för att tillhandahålla allmänna handlingar. Vidare rekommenderas domstolarna att överväga om gallring av uppgifter i Vera kan göras tidigare än enligt de gallringsfrister som föreskrivs i Vera-förordningarna. Kort efter beslutet från Datainspektionen stängde Domstolsverket besöksterminalerna vid samtliga domstolar.

Exemplet med besöksterminaler illustrerar den motsättning som finns mellan offentlighetsprincipen och intresset av att skydda den personliga integriteten. Det är viktigt att effekterna för den personliga integriteten beaktas när man avgör på vilket sätt behovet av insyn ska tillgodoses. Det är naturligtvis också av stor vikt att personuppgiftsbehandlingen görs i enlighet med gällande reglering och att t.ex. känsliga personuppgifter inte förekommer i diarium utan stöd i författning.

17.3 Behandling av uppgifter i ljud- och bildupptagning

17.3.1 Företeelsen

Sedan 2008 dokumenteras förhör vid tingsrätt som huvudregel genom ljud- och bildupptagning i Vera. En berättelse som lämnas i högre rätt får dokumenteras på samma sätt, men detta görs vanligtvis endast genom en ljudinspelning.

[7] Datainspektionens beslut den 30 september 2014 (dnr 1316-2013, 1317-2013, 1318-2013 och 1319-2013).

17.3.2 Det skyddande regelverket

Enligt 6 kap. 6 § rättegångsbalken ska tingsrätten som huvudregel dokumentera förhör som hålls i bevissyfte genom en ljud- och bildupptagning. För att tingsrätten inte ska dokumentera förhöret på detta sätt krävs att det finns särskilda skäl mot det. Undantaget avser framför allt det fall att en upptagning av något skäl kan försämra utredningen i målet eller situationer då tekniken för inspelning av någon anledning inte finns tillgänglig.

Bedömningen av om det finns skäl att avstå från att göra en ljud- och bildupptagning ska göras med beaktande av den sekretessbestämmelse som gäller i fråga om bilduppgiften. Av 43 kap. 4 § offentlighets- och sekretesslagen följer att sekretess gäller för själva bilduppgiften i en ljud- och bildupptagning, om det inte står klart att uppgiften kan röjas utan att den hörde lider men. Den som förhörs har alltså ett sådant skydd mot att bilduppgiften sprids, att utrymmet för att låta bli att dokumentera ett förhör genom en ljud- och bildupptagning av hänsyn till integritets- och utredningsskäl anses vara mycket begränsat.[8]

I rättsfallet NJA 2008 s. 883 förklarade Högsta domstolen att en part har en ovillkorlig rätt att ta del av en bildupptagning, men att det är en lämplighetsfråga om parten ska få ta del av upptagningen hos en domstol eller genom ett utlämnande av en kopia. Enligt Högsta domstolen är det inte lämpligt att en part får en kopia av bildupptagningen som parten kan behålla, kopiera eller sprida, om parten på ett rimligt sätt kan ta del av bildupptagningen på annat sätt, t.ex. genom ett besök hos en domstol. Som utgångspunkt gäller alltså att bildupptagningar inte lämnas ut från domstolen.

Ljud- och bildupptagningarna från tingsrättens förhandling ska gallras senast sex veckor efter det att målet eller ärendet har avgjorts genom dom eller beslut som har vunnit laga kraft (20 § förordningen [1996:271] om mål och ärenden i allmän domstol).

[8] Regeringens proposition *En modernare rättegång – reformering av processen i allmän domstol*, prop. 2004/05:131 s. 228 f.

17.3.3 Risker för den personliga integriteten

Det har många fördelar att förhör filmas. Framför allt innebär det att hovrätterna får ett bättre underlag än vad enbart ljudupptagningar ger när det gäller att bedöma bevisvärdet av förhör som hållits i tingsrätten. Det medför också att antalet omförhör i hovrätt kan begränsas, vilket är till fördel för såväl för domstolen som för vittnen och andra förhörspersoner som inte behöver inställa sig i domstol på nytt. I många fall är det en fördel om tingsrättsförhöret läggs fram i hovrätten genom en videoupptagning i stället för att förhörspersonen hörs på nytt, eftersom berättelsen i tingsrätten, som lämnas i närmare anslutning till den aktuella händelsen än en berättelse i hovrätten, i många fall ger ett bättre uttryck för vittnets verkliga iakttagelser.[9]

Vid förhör i domstol lämnas dock personuppgifter som många gånger kan vara känsliga. En inspelning av förhöret med ljud och bild kan vara mycket närgången. Den sekretess som gäller för dessa inspelningar är därför av stor betydelse. Om bildupptagningar av förhören lämnades ut kan det innebära en betydande risk för att dessa skulle spridas på exempelvis internet. Utöver den integritetskränkning som detta kan innebära, skulle det sannolikt ha negativ påverkan på viljan att lämna känsliga uppgifter under förhören.

Av nämnda skäl är det även viktigt att undvika obehörig spridning av uppgifterna internt på domstolarna, t.ex. genom att anställda av nyfikenhet tar del av ljud- och bildupptagningar som de inte behöver se för att utföra någon arbetsuppgift. Denna risk kan begränsas bl.a. genom loggning och uppföljning av loggningen. Som tidigare nämnts ska tillgången till personuppgifter enligt domstolsdatalagen begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.

[9] Se vidare prop. 2004/05:131 s. 106 f.

17.4 Informationsutbyte mellan domstolar och andra myndigheter

17.4.1 Företeelsen

Domstolarna och andra myndigheter har tidigare i huvudsak bytt information med varandra manuellt och pappersbaserat. Detta medförde att uppgifter om till exempel namn, personnummer, adress och brottslig gärning, registrerades på nytt ett stort antal gånger hos olika myndigheter. Mycket tid ägnades åt att kopiera, hantera och skanna in pappersdokument i de olika myndigheternas verksamhetssystem. För närvarande pågår arbete inom ramen för Rådet för rättsväsendets informationsförsörjning (RIF) som syftar till att skapa en helt elektronisk och strukturerad informationsförsörjning för rättsväsendets myndigheter. I en första etapp, som avslutades i december 2013, har ett elektroniskt informationsflöde skapats mellan de myndigheter som hanterar de största ärendemängderna i brottmålsprocessen, dvs. Rikspolisstyrelsen, Skatteverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Domstolsverket och Kriminalvården. Även Brottsförebyggande rådet får information, vilken den omvandlar till statistik. I den andra etappen deltar även Tullverket och Kustbevakningen. Det elektroniska kommunikationsflödet innebär att bl.a. förundersökningsprotokoll och uppgifter om inblandade aktörer överförs elektroniskt från polis till åklagare och vidare från åklagare till domstolar, med stora tidsvinster och besparingar som följd. Myndigheterna som ingår i den första etappen har fattat överenskommelser med varandra om informationsutbytet. I överenskommelsen regleras bl.a. frågor om ansvar och säkerhet. När det gäller säkerheten anges t.ex. att informationsutbytet ska göras via det statliga SGSI-nätet – där kommunikationen är krypterad och inte passerar internet – och att parterna ansvarar för att kommunikationen intrångsskyddas av brandväggar. Det ska också finnas spårbarhet och loggning ska göras enligt vissa krav.

17.4.2 Det skyddande regelverket

För att en myndighet ska få lämna ut sekretessbelagda uppgifter till en annan myndighet krävs att någon sekretessbrytande bestämmelse är tillämplig, t.ex. att myndigheten är skyldig att lämna ut uppgiften

eller att det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda (se framför allt 10 kap. offentlighets- och sekretesslagen). Eventuell överföring mellan myndigheter måste dessutom, precis som annan behandling, göras på ett säkert sätt (31 § personuppgiftslagen). Vidare är varje myndighet personuppgiftsansvarig för sin respektive behandling av uppgifterna, även om uppgifterna har lagts in i en myndighets datasystem av någon annan myndighet. Den personuppgiftsansvarige ska bl.a. säkerställa att myndigheten inte behandlar fler uppgifter än vad som är nödvändigt med hänsyn till ändamålen, att de uppgifter som behandlas är riktiga och, om det är nödvändigt, att de är aktuella och att alla rimliga åtgärder vidtas för att rätta, blockera, eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Uppgifterna ska dessutom behandlas på ett korrekt sätt i enlighet med god sed (9 § första stycket, b personuppgiftslagen). Vad som är god sed vid behandling av personuppgifter får enligt förarbetena[10] avgöras i rättstillämpningen mot bakgrund av bl.a. de mer preciserade föreskrifter som kan meddelas med stöd av personuppgiftslagen, de branschregler på området som kan ha utarbetats av etablerade branschorganisationer eller andra representativa sammanslutningar och hur ansvarsfulla personuppgiftsansvariga som regel beter sig.

17.4.3 Risker för den personliga integriteten

Merparten av uppgifterna som överförs mellan myndigheterna är uppgifter som under alla förhållanden måste behandlas där. Det elektroniska flödet mellan myndigheterna medför dock att uppgifterna sprids snabbare, att de enskilda myndigheternas ansvar för uppgifterna riskerar att bli otydligare och att bedömningarna av om uppgifterna får behandlas kan bli svårare när uppgifterna levereras in i systemen mer eller mindre automatiskt. När det gäller denna typ av informationsbyte är det därför särskilt viktigt att det finns tydliga regler och rutiner för hur hanteringen ska gå till.[11] Den nya regleringen kan förväntas innebära förtydliganden i dessa avseenden.

[10] Regeringens proposition *Personuppgiftslag*, prop. 1997/98:44 s. 143.
[11] Datainspektionens rapport 2012:1, *Rättsväsendets informationsförsörjning och den personliga integriteten*.

17.5 Utlämnande av uppgifter på medium för automatiserad behandling

17.5.1 Företeelsen

Domstolarnas verksamhet innehåller många moment som innebär att personuppgifter lämnas ut, t.ex. skickas handlingar till parter och andra aktörer inom ramen för handläggningen av mål och ärenden. Vidare lämnas allmänna handlingar ut till allmänheten med stöd av offentlighetsprincipen, efter begäran av bl.a. privatpersoner, journalister, företag och organisationer. Utlämnandet kan göras på olika sätt, bl.a. i form av papperskopia av en av handling eller utskrift från dator. I allt större utsträckning lämnas handlingar också ut i elektronisk form, t.ex. per e-post eller på ett usb-minne.

17.5.2 Det skyddande regelverket

Framför allt de allmänna domstolarnas verksamhet präglas i stor utsträckning av den grundlagsfästa offentlighetsprincipen. Av 2 kap. 1 § tryckfrihetsförordningen följer att allmänna handlingar ska vara tillgängliga för alla och att domstolen har en skyldighet att lämna ut dem till allmänheten. Som framgår under avsnitt 17.1.3 gäller sekretess i vissa fall även hos domstol, bl.a. avseende enskildas personliga förhållanden. Sekretess hindrar dock i de flesta fall inte att parter i ett mål eller ärende tar del av uppgifter.

Av offentlighetsprincipen följer endast en rätt att få ut en kopia av en allmän handling i pappersform. Domstolarna är alltså inte skyldiga att lämna ut handlingar i elektronisk form, även om så många gånger görs som en serviceåtgärd. I personuppgiftslagen regleras inte heller särskilt på vilket sätt som personuppgifter får lämnas ut.

E-post som skickas som ett led i ärendehanteringen, och som ingår i domstolens mål- och ärendehanteringssystem, anses vara en behandling av personuppgifter som fullt ut omfattas av regleringen i personuppgiftslagen. Viss annan e-postkorrespondens, exempelvis svar på frågor från allmänheten, anses däremot vara ostrukturerat material som enligt 5 a § personuppgiftslagen endast i begränsad

omfattning omfattas av nämnda reglering.[12] Det generella kravet på informationssäkerhet enligt 31 § personuppgiftslagen gäller dock även för sådan e-post.

Enligt domstolsdatalagen får personuppgifter endast lämnas ut på medium för automatiserad behandling om det inte är olämpligt. I författningskommentaren anges att en prövning av lämpligheten ska göras i varje enskilt fall och att det har betydelse vem mottagaren är. Lämplighetsprövningen blir särskilt viktig när uppgifterna ska lämnas till enskild och det på grund av personuppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet i förlängningen kan leda till integritetsrisker. Som exempel nämns att försiktighet är påkallad när det är fråga om fotografier eller ljudupptagningar samt uppgifter som är sammanställda utifrån en sökning som framstår som integritetskänslig.[13] I lagen upplyses vidare om möjligheten för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

17.5.3 Risker för den personliga integriteten

Utlämnande av handlingar som innehåller personuppgifter görs många gånger i elektronisk form med hjälp av e-post. Det är naturligt eftersom uppgifter i allt högre grad skapas och eller lagras i domstolarnas datorsystem. För allmänheten förenklar och effektiviserar det tillgången till domstolarnas offentliga information, vilket i sig ökar möjligheterna till insyn och kontroll. Domstolarna kan inte heller vägra att ta emot handlingar som kommer via e-post. För parter och andra aktörer, inklusive domstolen, innebär det många gånger en förenkling och kostnadsbesparing att kommunicera per e-post.

Ett utlämnande av uppgifter i elektronisk form innebär dock särskilda risker från integritetssynpunkt. Den elektroniska formen innebär som regel större möjligheter för mottagaren att på olika sätt bearbeta uppgifter – t.ex. genom strukturering och samkörning med

[12] Datainspektionens yttrande den 16 augusti 2012, dnr 1020-2012, och Domstolsverkets riktlinjer om e-posthantering, dnr 937-2009, s. 7 f.
[13] Prop. 2014/15:148 s. 113 f.

andra uppgifter – och att sprida informationen, än om utlämnande görs på papper.[14] Det kan t.ex. göra det möjligt för enskilda att sammanställa uppgifter till egna belastningsregister och dylikt (jfr 21 § personuppgiftslagen om att uppgifter om lagöverträdelse m.m. endast får behandlas av myndighet). I detta sammanhang kan också pekas på bestämmelsen i 21 kap. 7 § offentlighets- och sekretesslagen, som innebär att sekretess gäller för personuppgift om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen.

Mot den bakgrunden är det viktigt att ett utlämnande i elektronisk form endast görs när detta bedöms vara lämpligt, dvs. när det inte finns några tecken på att uppgifterna kommer att missbrukas, och att överföringen görs på ett säkert sätt.[15] När det handlar om strukturerat material är det också viktigt att man uppmärksammar bl.a. förbudet mot tredjelandsöverföring.

Ett särskilt problem som uppmärksammats är tillhandahållandet av personuppgifter på internet, som blivit allt vanligare. Det förekommer bl.a. webbplatser där det publiceras inkomstuppgifter och uppgifter om brottmålsdomar i stor omfattning. I många fall omfattas verksamheterna av den så kallade databasregeln i 1 kap. 9 § yttrandefrihetsgrundlagen. Den bestämmelsen reglerar under vilka förutsättningar tillhandahållande av information från en databas över internet omfattas av lagen. Bestämmelserna i personuppgiftslagen, som bl.a. förbjuder andra än myndigheter att behandla uppgifter om lagöverträdelse, tillämpas inte i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Detta medför att personuppgiftslagens regler till skydd för den personliga integriteten i praktiken inte gäller för den som har utgivningsbevis och därmed grundlagsskydd för sin databas. Tanken med utgivningsbevis var ursprungligen att främst skydda nya former av massmedial verksamhet. Vid en ansökan om utgivningsbevis görs det dock inte någon prövning av databasens innehåll eller syfte. Det går alltså att få grundlagsskydd även för databaser som inte har någon massmedial karaktär.

[14] *Domstolsdatalag*, Ds 2013:10 s. 117 f.
[15] *Domstolsverkets riktlinjer för e-posthantering*, dnr 937-2009; yttrande från Datainspektionen, *Samråd om domstolarnas e-posthantering*, dnr 1020-2012.

Mediegrundlagskommittén har fått i uppdrag att analysera vilka konflikter med skyddet för den personliga integriteten som uppkommer när information tillhandahålls ur databaser med utgivningsbevis och att ta ställning till om förändringar behövs för att tillgodose integritetsskyddet. I direktiven anges att kommittén i sin analys ska göra en noggrann avvägning mellan intresset av yttrandefrihet och intresset att skydda enskildas personliga integritet. Vidare ska utgångspunkten vara att det även fortsättningsvis ska finnas möjlighet att få grundlagsskydd genom utgivningsbevis. Uppdraget ska redovisas senast den 1 september 2016.[16]

17.6 Kommitténs samlade bedömning av området

I domstolarna behandlas en stor mängd uppgifter som rör enskildas personliga förhållanden. I många mål- och ärendetyper är det fråga om känsliga personuppgifter. Det ligger dessutom i sakens natur att domstolarna har mycket begränsade möjligheter att själva avgöra vilka personuppgifter som ska behandlas där. Om en part ger in ett dokument till domstolen, är domstolen – oavsett handlingens innehåll – i regel skyldig att registrera handlingen och kommunicera den med motparten. Även den enskilde har i många fall begränsade möjligheter att påverka vilka personuppgifter som behandlas i domstolen.

Det finns ett starkt intresse av att säkerställa att allmänheten har goda möjligheter till insyn i domstolarnas rättsvårdande och rättsskipande verksamhet. Medborgarna tycks också förvänta sig en enkel tillgänglighet, på samma sätt som när det gäller kontakter med andra aktörer i samhället. Det finns även ett starkt intresse av att domstolarnas verksamhet bedrivs effektivt, så att domar och beslut kan meddelas inom rimlig tid. Allt detta förutsätter bl.a. en ändamålsenlig användning av modern teknik.

I detta kapitel om integritetsrisker som hör ihop med domstolarnas hantering av personuppgifter har kommittén framför allt behandlat riskerna med verksamhetsregister, besöksterminaler, filmade förhör, informationsutbyte med andra myndigheter och utlämnande av uppgifter på medium för automatiserad behandling.

[16] Dir. 2014:97 *En kommitté på det tryck- och yttrandefrihetsrättsliga området.*

Verksamhetsregister

En risk med domstolarnas verksamhetsregister är att fler uppgifter än nödvändigt behandlas i registren och att känsliga personuppgifter behandlas på ett felaktigt sätt. Från och med januari 2016 finns dock en lag som reglerar domstolarnas behandling av personuppgifter. Kommittén bedömer att det finns en viss risk för att behandling av personuppgifter i domstolarnas verksamhetsregister leder till intrång i den personliga integriteten.

Ljud- och bildupptagningar

Risken med ljud- och bildupptagningar i domstol är att känsliga uppgifter sprids till obehöriga. Om en sådan upptagning lämnas ut i strid mot den sekretess som gäller, skulle uppgifterna enkelt kunna spridas på internet. Det finns också risker för att personal som inte är behörig tar del av upptagningarna av nyfikenhet. Det finns dock sekretessbestämmelser som skyddar uppgifterna. I domstolsdatalagen finns bestämmelser om att tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Kommittén bedömer att det finns en viss risk för intrång i den personliga integriteten i samband med ljud- och bildupptagningar i domstol.

Digitalt informationsutbyte med andra myndigheter

Risken för kränkningar av den personliga integriteten i samband med domstolarnas informationsutbyte med andra myndigheter inom rättsväsendet består i att känsliga uppgifter kan spridas till obehöriga inom eller utanför myndigheterna. Varje deltagande myndighet måste ansvara för sin behandling och upprätthålla rätt säkerhetsnivå. Domstolsdatalagen reglerar under vilka förutsättningar direktåtkomst till domstolens personuppgifter är tillåten. Kommittén bedömer att det finns en viss risk för intrång i den personliga integriteten i samband med detta informationsutbyte.

Utlämnande av uppgifter på medium för automatiserad behandling

Vid utlämnande av uppgifter i elektronisk form, per e-post eller på ett usb-minne finns det en risk för att känsliga personuppgifter kan spridas till obehöriga. Den elektroniska formen innebär större möjligheter för mottagaren att på olika sätt bearbeta uppgifter och sprida informationen än om utlämnande görs på papper.[17] Det kan t.ex. göra det möjligt för enskilda att sammanställa uppgifter till egna belastningsregister. Kommittén bedömer att det föreligger påtagliga risker för intrång i den personliga integriteten i samband med utlämnande av uppgifter på medium för automatiserad behandling.

Skydda integriteten med sekretess

En viktig del i skyddet för den personliga integriteten är möjligheterna att låta sekretess gälla för vissa uppgifter om enskilda. En alltför långtgående offentlighet kan medföra skador på såväl enskilda som allmänna intressen. Intresset av offentlighet i domstol måste exempelvis vägas mot rätten till skydd för privat- och familjeliv enligt artikel 8 i Europakonventionen. En konsekvens av en långtgående offentlighet kan också bli att domstolarna av integritetsskäl låter bli att i sina avgöranden närmare gå in på vissa uppgifter som är av betydelse i målet. Därigenom riskeras att en ofullständig bild ges av de skäl som lett domstolen fram till sitt ställningstagande, vilket i sin tur kan ha en negativ inverkan på medborgarnas förtroende för domstolarnas verksamhet.[18]

[17] *Domstolsdatalag*, Ds 2013:10 s. 117 f.
[18] Regeringens proposition *med förslag till sekretesslag*, prop. 1979/80:2 Del A, s. 102; se även Ds 2014:33 s. 37 f.

18 De brottsbekämpande myndigheternas verksamhet

Kommitténs bedömning: De olika företeelser som vi kartlagt inom området brottsbekämpning är förknippade med risker av olika allvarlighetsgrad: såväl vissa risker som påtagliga risker för den personliga integriteten kan konstateras. Läs mer om hur vi bedömt riskerna avseende de olika företeelserna i avsnitt 18.11.

18.1 Inledning

18.1.1 De brottsbekämpande myndigheternas användning av informationsteknik

Staten har en skyldighet att vidta effektiva åtgärder till skydd för den enskildes säkerhet. I detta ligger en skyldighet för staten att försöka förebygga och förhindra brott. Vidare krävs att brott utreds och att gärningsmän lagförs för brottsliga handlingar. Ansvaret för denna brottsbekämpande verksamhet ligger i första hand på Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten och Åklagarmyndigheten. Visst brottsbekämpande arbete bedrivs dock av andra myndigheter, exempelvis Tullverket.

För att fullgöra dessa uppgifter har de brottsbekämpande myndigheterna behov av olika typer av information, däribland personuppgifter och uppgifter om brott. Sådan information kan inhämtas genom exempelvis spaning och förhör eller genom användning av olika tvångsmedel. Information samlas i allt större utsträckning in med användning av informationsteknik. Ljud- och bildupptagningar samt tillgång till uppgifter om elektronisk kommunikation har blivit allt viktigare i myndigheternas underrättelse- och utredningsarbete.

Informationsteknik, bl.a. i olika former av datoriserade register, används också vid dessa myndigheters efterföljande behandling av insamlade uppgifter.

I detta kapitel behandlas ett antal företeelser inom de brottsbekämpande myndigheternas verksamhet som gäller informationsteknik och som är av särskild betydelse ur ett integritetsskyddsperspektiv. Kapitlet tar sin utgångspunkt i integritetsrisker för misstänkta personer. Flera av dessa risker kan dock även drabba andra personer, exempelvis vittnen och brottsoffer.

Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet behandlas i kapitel 19, *Försvarsunderrättelseverksamhet och militär underrättelsetjänst.*

18.1.2 Allmänt om den rättsliga regleringen

Den rättsliga reglering som är av störst betydelse i detta sammanhang är följande:

- I 8 § polislagen (1984:387) finns ett generellt krav på att en polisman, som har att verkställa en tjänsteuppgift under iakttagande av vad som föreskrivs i lag eller annan författning, ska ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Ett ingripande som begränsar någon av de grundläggande fri- och rättigheter som avses i 2 kap. regeringsformen får dock inte grundas enbart på en sådan bedömning.
- 27 kap. rättegångsbalken innehåller grundläggande bestämmelser om bl.a. beslag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning.
- Lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott innehåller bestämmelser som ger myndigheterna möjlighet att i förebyggande syfte använda bl.a. hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt hemlig kameraövervakning.
- Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet innehåller bestämmelser som bl.a. ger Polis-

myndigheten, Säkerhetspolisen och Tullverket vissa möjligheter att i underrättelseverksamhet i hemlighet hämta in uppgifter om elektronisk kommunikation för att förebygga, förhindra eller upptäcka viss allvarligare brottslig verksamhet.

- Lagen (1991:572) om särskild utlänningskontroll innehåller särskilda bestämmelser om användning av tvångsmedel i syfte att utreda om en utlänning eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.
- Lagen (2003:389) om elektronisk kommunikation innehåller bestämmelser om bl.a. tele- och internetoperatörers skyldighet att radera respektive lagra uppgifter om elektronisk kommunikation. Lagen innehåller även bestämmelser om att operatörerna har tystnadsplikt beträffande dessa uppgifter och om att de i vissa fall är skyldiga att lämna ut abonnemangsuppgifter till bl.a. Polismyndigheten.
- Lagen (2000:562) om internationell rättslig hjälp i brottmål innehåller bestämmelser om rättslig hjälp i brottmål i Sverige och utomlands, bl.a. när det gäller användning av hemliga tvångsmedel.
- Polisdatalagen (2010:361), lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister, lagen (2010:362) om polisens allmänna spaningsregister och personuppgiftslagen (1998:204) innehåller förhållandevis detaljerade regler om polisens behandling av personuppgifter.

Under de senaste åren har det genomförts ett stort antal lagändringar på detta område som bl.a. har syftat till att åstadkomma en bra balans mellan behovet av en effektiv brottsbekämpning och skyddet för den

personliga integriteten.[1] Vissa av dessa lagstiftningsåtgärder har föregåtts av en omfattande kartläggning av de brottsbekämpande myndigheternas behov och nytta av vissa tvångsmedel.[2]

Polismetodutredningen har i sitt betänkande[3] föreslagit att det, som ett komplement till det allmänna proportionalitetskravet i 8 § polislagen, ska införas en ny lag om särskilda inhämtningsåtgärder i de brottsbekämpande myndigheternas verksamhet. Lagen föreslås bl.a. innehålla bestämmelser om när polisen får använda dolda kroppsmikrofoner, handmanövrerade kameror och s.k. pejling. Förslaget i den delen syftar till att stärka den personliga integriteten och innebär bl.a. att upptagning med sådan utrustning endast får förekomma dels i förundersökning om åtgärden kan antas vara av särskild betydelse för utredning av brott för vilket är föreskrivet fängelse i ett år eller däröver, dels i underrättelseverksamhet om det finns särskild anledning att anta att åtgärden kan bidra till att förebygga, förhindra eller upptäcka brott av angivet slag.

18.1.3 Tillsyn

Datainspektionen har det övergripande ansvaret för att värna skyddet för enskildas personliga integritet såvitt avser behandling av personuppgifter i den brottsbekämpande verksamheten. Post- och telestyrelsen har i uppdrag att utöva tillsyn över att tjänsteleverantörerna följer lagen om elektronisk kommunikation och skyldigheten att lagra vissa uppgifter för brottsbekämpande ändamål.

Vidare har Säkerhets- och integritetsskyddsnämnden enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet i uppgift att utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel. Säkerhets- och integritetsskyddsnämnden har även tillsyn över polisens behandling av personuppgifter enligt polisdatalagen och lagen om polisens allmänna spaningsregister. Nämnden är också skyldig att på begäran av enskild kontrollera om han eller hon har varit föremål för polisens personuppgiftsbe-

[1] Regeringens proposition *Integritet och effektivitet i polisens brottsbekämpande verksamhet*, prop. 2009/10:85, Regeringens proposition *De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation*, prop. 2011/2012:55 och Regeringens proposition om *Hemliga tvångsmedel mot allvarliga brott*, prop. 2013/14:237.

[2] Utredningens om vissa hemliga tvångsmedel betänkande *Hemliga tvångsmedel mot allvarliga brott*, SOU 2012:44.

[3] Polismetodutredningens betänkande *Särskilda spaningsmetoder*, SOU 2010:103.

handling och om personuppgifter har behandlats i enlighet med lag eller annan författning. Säkerhets- och integritetsskyddsnämnden utför kontroller på begäran av enskilda när det gäller hemliga tvångsmedel och därmed sammanhängande verksamhet. Om nämnden i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten eller annan behörig myndighet. Vidare ska nämnden om man finner omständigheter som Datainspektionen bör uppmärksammas på, anmäla det till inspektionen.

Justitiekanslern ska pröva anmälningar från Säkerhets- och integritetsskyddsnämnden om felaktigheter som kan medföra skadeståndsansvar för staten. Dessutom har Justitiekanslern och Riksdagens ombudsmän (Justitieombudsmannen) till uppgift att utöva tillsyn bl.a. över myndigheternas användning av tvångsmedel och behandling av personuppgifter.

18.2 Hemlig rumsavlyssning och annan ljudupptagning som inte avser elektronisk kommunikation

18.2.1 Företeelsen

I de brottsbekämpande myndigheternas underrättelse- och utredningsverksamhet används mikrofoner och därmed jämförbar utrustning för att avlyssna eller spela in ljud.

Utöver hemlig rumsavlyssning av angivet slag förekommer det att exempelvis en polis, eller någon som samarbetar med polisen, använder en dold kroppsmikrofon eller annan liknande utrustning för att spela in, eller för att låta någon annan direkt ta del av ett samtal som denne själv deltar i, trots att någon eller några av de andra personerna som deltar i samtalet är ovetande om inspelningen eller avlyssningen.

18.2.2 Det skyddande regelverket

När det gäller inspelning eller avlyssning med dold kroppsmikrofon eller liknande är utgångspunkten att var och en som deltar i ett samtal (eller i ett sammanträde) i princip kan förfoga över detsamma och tillåta t.ex. avlyssning eller ljudupptagning. Det finns inte heller

någon reglering som specifikt tar sikte på polisens rätt att få ägna sig åt sådan verksamhet. Av den generella regleringen i 8 § polislagen – som gäller för all utövning av polisiära tvångsbefogenheter – följer dock att en polisman, som har att verkställa en tjänsteuppgift under iakttagande av vad som föreskrivs i lag eller annan författning, ska ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Dessutom sätter polisdatalagen vissa yttre gränser för behandlingen av ljudupptagningar.[4]

De brottsbekämpande myndigheternas möjligheter att använda hemlig rumsavlyssning är däremot särskilt reglerat i 27 kap. rättegångsbalken. Med hemlig rumsavlyssning avses avlyssning eller upptagning i hemlighet och med hjälp av tekniskt hjälpmedel som är avsett att återge ljud, och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, som allmänheten inte har tillträde till. Regleringen tar alltså sikte på situationer där ingen av de som deltar i samtalet eller sammankomsten har samtyckt till avlyssningen eller upptagningen (jfr 4 kap. 9 a § brottsbalken).

Av regleringen framgår bl.a. att hemlig rumsavlyssning alltid kräver tillstånd av domstol och att enskildas integritetsintressen tillvaratas av ett offentligt ombud. Tillstånd för hemlig rumsavlyssning får meddelas endast när någon är skäligen misstänkt för ett brott som har ett minimistraff om fyra års fängelse samt vid viss annan allvarlig brottslighet. Ett beslut om hemlig rumsavlyssning förutsätter vidare att åtgärden är av synnerlig vikt för utredningen samt att skälen för åtgärden uppväger det intrång eller men i övrigt som den innebär för den misstänkte eller för något annat motstående intresse.

Det finns också begränsningar beträffande var rumsavlyssning får användas, på vilket sätt uppgifter som kommit fram vid avlyssningen får användas och hur länge de får bevaras m.m.

Av betydelse för den personliga integriteten är även att regleringen innehåller bestämmelser om hur länge ett tillstånd får gälla, om utformningen av besluten och om underrättelse till den misstänkte i efterhand.

[4] Säkerhets- och integritetsskyddsnämndens uttalande den 4 september 2013, dnr 84-2013, angående behandling av personuppgifter i uppgiftssamlingar med spaningsfilmer.

18.2.3 Risker för den personliga integriteten

Hemlig rumsavlyssning gör det möjligt att få veta vad som sägs vid privata sammankomster, exempelvis hemma hos någon av de misstänkta. Detta tvångsmedel är därför ett viktigt komplement till andra hemliga tvångsmedel och anses ha stor betydelse för möjligheterna att utreda framför allt grov organiserad brottslighet. Det hänger samman med att den typen av gärningsmän ofta är riskmedvetna och väl insatta i hur myndigheterna arbetar. En effektiv utredning av bl.a. grov organiserad brottslighet förutsätter att de brottsbekämpande myndigheterna kan samla in information på många olika sätt, t.ex. information om vad misstänkta säger till varandra vid privata sammankomster, och sammanställa denna information.

Samtidigt är hemlig rumsavlyssning ett tvångsmedel vars användning i stort sett alltid innebär beaktansvärda integritetsintrång, särskilt när åtgärden riktas mot privat miljö som t.ex. bostäder. Avlyssningen omfattar många gånger allt som utspelar sig i det avlyssnade rummet, dvs. även samtal om känsliga frågor som helt saknar betydelse för brottsutredningen eller till och med gäller någon annan än den misstänkte.

Möjligheten till hemlig rumsavlyssning är dock begränsad till allvarlig brottslighet och omgärdas av ett antal funktioner som skyddar den personliga integriteten, t.ex. krav på domstolsprövning och offentliga ombud samt begränsningar av den krets som får granska upptagningen eller uppteckningen. Det sistnämnda minskar risken för oönskad spridning av insamlade uppgifter. Regleringen innehåller även bestämmelser om underrättelse i efterhand som framstår som väl avvägda. Dessutom finns, utöver den allmänna tillsyn som utövas av bl.a. Datainspektionen, SIN som har särskilt ansvar för tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel.

Även avlyssning eller inspelning med hjälp av exempelvis dolda kroppsmikrofoner kan leda utredningar framåt och innebära att viktiga bevis säkras, särskilt i arbetet mot organiserad brottslighet. Metoden kan dessutom utgöra ett skydd för den som bär mikrofonen, eller användas för att den som leder en viss spaningsoperation, av rättssäkerhetsskäl eller av operativa skäl, ska kunna följa händelseutvecklingen.

Inspelningar som görs med dolda kroppsmikrofoner och motsvarande utrustning kan innebära ett allvarligt integritetsintrång, även om de uppgifter som lämnas i sådana sammanhang i vissa fall kan antas vara något mindre integritetskänsliga än de uppgifter som är åtkomliga genom hemlig rumsavlyssning. En viktig skillnad är att en inspelning med dold kroppsmikrofon endast fångar upp ljud i polisens närhet, medan en hemlig rumsavlyssning omfattar allt som händer i exempelvis en bostad. Av betydelse i sammanhanget är även att inspelning med dold kroppsmikrofon inte omfattas av brottsbalkens förbud mot olovlig avlyssning.

18.3 Hemlig kameraövervakning och annan bildupptagning

18.3.1 Företeelsen

I de brottsbekämpande myndigheternas underrättelse- och utredningsverksamhet används videokameror och därmed jämförbar utrustning för optisk personövervakning.

18.3.2 Det skyddande regelverket

De brottsbekämpande myndigheternas användning av hemlig kameraövervakning regleras i första hand i 27 kap. rättegångsbalken. Hemlig kameraövervakning innebär att fjärrstyrda videokameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar används för optisk personövervakning vid förundersökning i brottmål, utan att upplysning om övervakningen lämnas. Regleringen omfattar alltså inte ljudupptagningar och inte heller optisk personövervakning med utrustning som inte är fjärrstyrd.

Av regleringen framgår att hemlig kameraövervakning i princip kräver domstols tillstånd, men att åklagare i vissa brådskande situationer får ge ett tillstånd som i efterhand underställs domstolens prövning, samt att enskildas integritetsintressen tillvaratas genom ett offentligt ombud.

Tillstånd för hemlig kameraövervakning får meddelas endast vid förundersökning angående brott med ett miniminstraff om två års fängelse samt vid viss annan allvarlig brottslighet. Det krävs vidare

att åtgärden är av synnerlig vikt för utredningen. Kameraövervakning får endast avse en plats där den misstänkte kan antas komma att uppehålla sig eller, om det inte finns någon som är skäligen misstänkt för brottet, den plats där brottet har begåtts eller en nära omgivning till denna plats. Ett beslut om hemlig kameraövervakning förutsätter dessutom att skälen för åtgärden uppväger det intrång eller men i övrigt som den innebär för den misstänkte eller för något annat motstående intresse.

Det regleras också på vilket sätt uppgifter som kommit fram vid en hemlig kameraövervakning får användas och hur länge de får bevaras.

Av betydelse för den personliga integriteten är även att regleringen innehåller bestämmelser om hur länge ett tillstånd får gälla, om utformningen av besluten och om underrättelse till den misstänkte – eller till Säkerhets- och integritetsskyddsnämnden – i efterhand. Dessutom ska det i beslutet, när det finns skäl för det, anges övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Det kan exempelvis föreskrivas att övervakning av en lokal som även disponeras av andra endast får göras när man genom fysisk spaning kan konstatera att den misstänkte befinner sig där.

Vissa ytterligare möjligheter att använda hemlig kameraövervakning följer av lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Den regleringen innebär i korthet att hemlig kameraövervakning får användas även i förebyggande syfte, om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet av särskilt allvarligt slag (t.ex. sabotage, mordbrand, högförräderi, spionerі och terroristbrott). Detsamma gäller om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Det förekommer även att de brottsbekämpande myndigheterna använder exempelvis handmanövrerade kameror för optisk personövervakning. Sådan övervakning omfattas inte av den reglering som har beskrivits ovan. Det finns inte heller någon annan lagstiftning som tar sikte på användningen av sådana hjälpmedel. Av den generella regleringen i 8 § polislagen följer dock att en polisman som har

att verkställa en tjänsteuppgift under iakttagande av vad som föreskrivs i lag eller annan författning, ska ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Dessutom sätter polisdatalagen vissa yttre gränser för behandlingen av bildupptagningar.[5]

Användningen av kameraövervakning för andra syften än brottsbekämpning behandlas i kapitel 20 *Övervakning med kamera*.

18.3.3 Risker för den personliga integriteten

Hemlig kameraövervakning anses vara ett mycket effektivt verktyg vid utredning av allvarliga brott, i och med att det ger en möjlighet för de brottsbekämpande myndigheterna att iaktta och spela in misstänkta brottslingars agerande. Vid sådan brottslighet är det också – med hänsyn till att gärningsmännen ofta är säkerhetsmedvetna och har god kunskap om hur myndigheterna arbetar – av stor vikt att myndigheterna kan samla in information på många olika sätt och sammanställa denna information.

Även användningen av exempelvis handmanövrerade kameror kan leda utredningar framåt och innebära att viktiga bevis säkras, särskilt i arbetet mot organiserad brottslighet. Användningen av sådan utrustning kan dessutom – på samma sätt som exempelvis dolda kroppsmikrofoner – utgöra ett skydd för den som bär utrustningen, eller användas för att den som leder en viss spaningsoperation, av rättssäkerhetsskäl eller av operativa skäl, ska kunna följa händelseutvecklingen.

Samtidigt är hemlig kameraövervakning ett tvångsmedel vars användning innebär beaktansvärda integritetsintrång, särskilt när åtgärden riktas mot privat miljö som exempelvis bostäder. Den plats som övervakningen avser kan dessutom besökas eller passeras av andra personer än den misstänkte. En person, som inte är misstänkt för brott, som kan komma att filmas kan ha personliga skäl till att andra inte ska veta var han eller hon befinner sig.

[5] Säkerhets- och integritetsskyddsnämndens uttalanden den 11 december 2012 (dnr 177-2012) respektive den 4 september 2013 (dnr 84-2013), angående behandling av personuppgifter i uppgiftssamlingar med spaningsfilmer.

Möjligheten till hemlig kameraövervakning är dock begränsad till allvarlig brottslighet och omgärdas av ett antal funktioner som skyddar den personliga integriteten, t.ex. krav på domstolsprövning och offentliga ombud samt begränsningar av den krets som får granska upptagningen eller uppteckningen. Det sistnämnda minskar risken för oönskad spridning av insamlade uppgifter. Det finns även bestämmelser om underrättelse i efterhand som framstår som väl avvägda. Dessutom finns den särskilda tillsynen som SIN utövar.

18.4 Hemlig avlyssning av elektronisk kommunikation

18.4.1 Företeelsen

Brottsbekämpande myndigheter kan i hemlighet avlyssna innehållet i telefonsamtal och andra meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät, exempelvis sms och e-post.

Lagen skiljer på hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation, som vi behandlar i nästföljande avsnitt.

Hemlig avlyssning av elektronisk kommunikation innebär enligt 27 kap. 18 § RB att sådana meddelanden avlyssnas i hemlighet eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.

18.4.2 Det skyddande regelverket

De brottsbekämpande myndigheternas användning av hemlig avlyssning av elektronisk kommunikation, dvs. myndigheternas möjligheter att i hemlighet avlyssna eller ta upp innehållet i meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät till eller från ett telefonnummer eller annan adress, regleras i första hand i 27 kap. rättegångsbalken.

Av regleringen framgår att hemlig avlyssning av elektronisk kommunikation i princip kräver domstols tillstånd, men att åklagare i vissa brådskande situationer får ge ett tillstånd som i efterhand underställs domstolens prövning, samt att enskildas integritetsintressen tillvaratas genom ett offentligt ombud.

Tillstånd till hemlig avlyssning av elektronisk kommunikation får meddelas endast vid förundersökning angående brott med ett miniminstraff om två års fängelse samt vid viss annan allvarlig brottslighet. Det krävs dessutom att någon är skäligen misstänkt för brottet och att åtgärden är av synnerlig vikt för utredningen samt att skälen för åtgärden uppväger det intrång eller men i övrigt som den innebär för den misstänkte eller för något annat motstående intresse. Åtgärden får endast avse telefonnummer, adress eller kommunikationsutrustning som på visst närmare angivet sätt kan knytas till den misstänkte.

Det finns även vissa absoluta begränsningar av vilken elektronisk kommunikation som får avlyssnas. Avlyssning får t.ex. inte avse samtal eller tal där exempelvis en advokat eller läkare deltar, som inte hade kunnat höras som vittne om det som framkommit.

Det regleras också hur uppgifter som kommer fram vid en hemlig avlyssning av elektronisk kommunikation får användas.

Om det är åklagaren som har gett tillstånd till hemlig avlyssning av elektronisk kommunikation och rätten vid sin efterföljande prövning av ett verkställt beslut finner att det inte borde ha getts tillstånd, får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av avlyssningen, eller för någon annan som uppgifterna avser. I övrigt gäller att en upptagning eller uppteckning som har gjorts vid hemlig avlyssning av elektronisk kommunikation ska granskas snarast möjligt. Granskningen får i princip bara göras av undersökningsledaren, åklagaren eller rätten. I de delar som upptagningarna eller uppteckningarna är av betydelse från brottsutredningssynpunkt, ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna eller uppteckningarna är av betydelse för att förhindra förestående brott, ska de bevaras så länge det behövs för att förhindra brott. Upptagningarna eller uppteckningarna ska därefter förstöras. Om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis polisdatalagen eller lagen om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet, får dock uppgifterna sparas och användas enligt dessa lagar. I den situationen gäller de särskilda lagarnas bestämmelser om gallring med mera.

Av betydelse för den personliga integriteten är även att regleringen innehåller bestämmelser om hur länge ett tillstånd får gälla, om utformningen av besluten och om underrättelse till den misstänkte – eller till SIN – i efterhand. Dessutom ska det i beslutet, när det finns skäl för det, anges övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Det kan exempelvis föreskrivas att avlyssning av utrustning som även disponeras av andra, exempelvis datorer på ett bibliotek, endast får göras när man genom fysisk spaning kan konstatera att den misstänkte använder eller avser att använda utrustningen.

Ytterligare bestämmelser om hemlig avlyssning av elektronisk kommunikation finns i lagen (1991:572) om särskild utlänningskontroll och lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

Enligt lagen om särskild utlänningskontroll får domstol, om det föreligger synnerliga skäl, ge de brottsbekämpande myndigheterna tillstånd till hemlig avlyssning av elektronisk kommunikation för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott.

Regleringen i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott innebär, såvitt här är av intresse, i korthet att hemlig avlyssning av elektronisk kommunikation får användas även i förebyggande syfte, om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet av särskilt allvarligt slag (t.ex. sabotage, mordbrand, högförräderi, spionerі och terroristbrott). Detsamma gäller om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet av angivet slag och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Generellt gäller att ett tillstånd till hemlig avlyssning av elektronisk kommunikation också ger rätt att inhämta uppgifter om den elektroniska kommunikationen genom hemlig övervakning av elektronisk kommunikation.

18.4.3 Risker för den personliga integriteten

Hemlig avlyssning av elektronisk kommunikation anses vara ett mycket värdefullt verktyg, särskilt i utredningar om allvarlig brottslighet.

Utöver den kartläggning av kontaktnät och rörelsemönster som bl.a. hemlig övervakning av elektronisk kommunikation kan ge, så kan hemlig avlyssning ge mer konkret information om t.ex. innehållet i brottsplaner.[6] Det är dessutom av stor vikt att myndigheterna kan samla in information på många olika sätt och sammanställa denna information, särskilt vid organiserad brottslighet där gärningsmännen ofta är riskmedvetna och har god insikt i hur myndigheterna arbetar.

Samtidigt innebär hemlig avlyssning av elektronisk kommunikation att polisen lyssnar på vad den misstänkte och andra personer talar om i telefon eller tar del av vad de skriver i t.ex. sms- och e-postmeddelanden. Det ligger i sakens natur att en del av det som sägs eller skrivs inte är relevant för det brott som avlyssningen avser, utan kan gälla t.ex. familjeliv, ekonomi eller andra personliga förhållanden. Den känsliga informationen kan dessutom gälla någon annan än den misstänkte. Avlyssningen får därför anses utgöra ett stort intrång i enskildas personliga integritet.

Möjligheten till hemlig avlyssning av elektronisk kommunikation är dock begränsad till allvarlig brottslighet och omgärdas av ett förhållandevis stort antal rättssäkerhetsgarantier, t.ex. domstolsprövning, förekomsten av offentliga ombud och begränsningen av den krets som får granska upptagningen. Det sistnämnda är ägnat att minska risken för oönskad spridning av insamlade uppgifter, även om möjligheten att föra in och behandla uppgifterna i olika register riskerar att ge uppgifterna en vidare spridning. Det finns dessutom bestämmelser om underrättelse i efterhand som framstår som väl avvägda samt en tillsyn av användningen av detta tvångsmedel som såvitt kan bedömas är välfungerande. Vidare finns, som framhållits ovan, SIN som särskild tillsynsmyndighet när det gäller användningen av hemliga tvångsmyndigheter.

[6] SOU 2012:44, s. 491 f.

18.5 Hemlig övervakning av elektronisk kommunikation

18.5.1 Företeelsen

Leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster (exempelvis telefon- eller bredbandsabonnemang) och allmänna kommunikationsnät (exempelvis system för överföring av telefon- eller internettrafik) lagrar under viss tid bl.a. trafik- och lokaliseringsuppgifter samt uppgifter som behövs för att identifiera en abonnent eller användare. Dessa lagrade uppgifter är under vissa förutsättningar åtkomliga för de brottsbekämpande myndigheterna. Dessa myndigheter inhämtar också lokaliseringsuppgifter på annat sätt.

Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om

- meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress,
- vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller
- i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Hemlig avlyssning av elektronisk kommunikation har behandlats i föregående avsnitt.

18.5.2 Det skyddande regelverket

Lagring och gallring hos tjänsteleverantörerna

Vid användning av tele- och internettjänster lagras olika uppgifter automatiskt i relativt stor omfattning i datorer som tillhör inblandade tjänsteleverantörer. Det som lagras är i huvudsak uppgifter som, när de kombineras med information om vem som har ett visst abonnemang, gör det möjligt att se vem som har kontakt med vem och vid vilken tidpunkt (s.k. trafikuppgifter) samt var de då befinner

sig (s.k. lokaliseringsuppgifter). Vid överföring av exempelvis sms- och e-postkorrespondens lagras automatiskt och tillfälligt själva innehållet i meddelandet.

Enligt lagen om elektronisk kommunikation är huvudregeln att leverantören är skyldig att utplåna eller avidentifiera sådana uppgifter som avser användare eller abonnenter som är fysiska personer så snart uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande. Det finns dock flera undantag från denna huvudregel.

Utöver bestämmelser om att leverantörerna får lagra vissa uppgifter så länge de behövs för vissa interna ändamål, innehåller lagen en skyldighet för i princip alla leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra trafik-, lokaliserings- och abonnemangsuppgifter för brottsbekämpande ändamål under sex månader, räknat från den dag då kommunikationen avslutades.

Åtkomst till lagrade uppgifter för brottsbekämpning

De brottsbekämpande myndigheterna kan under förundersökning och i underrättelseverksamhet få tillgång till trafik- och lokaliseringsuppgifter samt abonnemangsuppgifter på olika sätt.

Trafik- och lokaliseringsuppgifter kan inhämtas genom hemlig övervakning av elektronisk kommunikation. Vid sidan av regleringen i 27 kap. rättegångsbalken finns bestämmelser om hemlig övervakning i lagen om särskild utlänningskontroll och lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Trafik- och lokaliseringsuppgifter får även inhämtas i underrättelseverksamhet enligt lagen om inhämtning av uppgifter om elektronisk kommunikation.

Vidare ger lagen om elektronisk kommunikation myndigheterna rätt att få del av abonnemangsuppgifter vid misstanke om brott.

Hemlig övervakning enligt 27 kap. rättegångsbalken

Av regleringen i rättegångsbalken framgår att hemlig övervakning av elektronisk kommunikation i princip kräver domstols tillstånd, men att åklagare i vissa brådskande situationer får ge ett tillstånd som i efterhand underställs domstolens prövning. Vidare framgår att tillstånd till hemlig övervakning av elektronisk kommunikation får

meddelas endast vid förundersökning angående brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader samt vid viss annan särskilt angiven brottslighet (bl.a. terroristbrott, dataintrång, narkotikabrott och barnpornografibrott som inte är ringa).

För att hemlig övervakning av elektronisk kommunikation ska tillåtas krävs att åtgärden är av synnerlig vikt för utredningen. Om övervakningen avser någon som är skäligen misstänkt för brottet får åtgärden endast avse ett telefonnummer eller en annan adress eller en viss kommunikationsutrustning som kan antas ha använts eller komma att användas av den misstänkte, eller ett telefonnummer eller annan adress eller kommunikationsutrustning som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta. Hemlig övervakning av elektronisk kommunikation får dock även användas i syfte att utreda vem som skäligen kan misstänkas för brottet. Även i detta fall krävs att åtgärden är av synnerlig vikt för utredningen. Ett beslut om hemlig övervakning av elektronisk kommunikation förutsätter dessutom att skälen för åtgärden uppväger det intrång eller men i övrigt som den innebär för den misstänkte eller för något annat motstående intresse.

Det är också reglerat på vilket sätt uppgifter som framkommit vid hemlig övervakning av elektronisk kommunikation får användas och hur länge de får bevaras.

Av betydelse för den personliga integriteten är även att regleringen innehåller bestämmelser om hur länge ett tillstånd får gälla, om utformningen av besluten och om underrättelse till den misstänkte – eller till SIN – i efterhand. Dessutom ska det i beslutet, när det finns skäl för det, anges övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Det kan exempelvis föreskrivas att övervakning av utrustning som även disponeras av andra, exempelvis datorer på ett bibliotek, endast är tillåtet när man genom fysisk spaning kan konstatera att den misstänkte använder eller avser att använda utrustningen.

Hemlig övervakning enligt lagen om särskild utlänningskontroll

Enligt lagen om särskild utlänningskontroll får domstol, om det föreligger synnerliga skäl, ge de brottsbekämpande myndigheterna tillstånd till hemlig övervakning av elektronisk kommunikation för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott.

Hemlig övervakning enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott

Regleringen i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott innebär, såvitt här är av intresse, i korthet att hemlig övervakning av elektronisk kommunikation får användas även i förebyggande syfte, om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet av särskilt allvarligt slag (t.ex. sabotage, mordbrand, högförräderi, spionerі och terroristbrott). Detsamma gäller om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet av angivet slag och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Tillgång till uppgifter enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) får Polismyndigheten, Säkerhetspolisen och Tullverket i underrättelseverksamhet i hemlighet från den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst hämta in trafik- och lokaliseringsuppgifter. För inhämtning enligt denna lag krävs inte något domstolsbeslut, utan beslutet fattas av myndigheten. Myndighetschefen får delegera beslutsrätten till en anställd vid myndigheten som har den

särskilda kompetens, utbildning och erfarenhet som behövs. En sådan anställd får dock inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon själv deltar i.

En förutsättning för ett beslut enligt inhämtningslagen är vidare att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år eller annars är av särskilt allvarligt slag (t.ex. sabotage, mordbrand, högförräderi, spioneri och terroristbrott). Det krävs även att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse. Om det vid inhämtning av uppgifter enligt denna lag kommer fram uppgifter om annan brottslig verksamhet än som omfattas av beslutet om inhämtning, får uppgifterna användas för att förhindra brott eller för att inleda en förundersökning. För att uppgifterna ska få användas i en förundersökning krävs däremot att det har meddelats ett tillstånd om hemlig övervakning av elektronisk kommunikation.

En uppteckning av uppgifter som inhämtats enligt inhämtningslagen ska granskas snarast möjligt. Uppteckningar ska, i de delar de är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet som omfattas av beslutet om inhämtning eller för att förhindra annat brott, bevaras så länge det behövs för något av dessa syften. De ska därefter förstöras. Om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis polisdatalagen eller lagen om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet, får dock uppgifterna sparas och användas enligt dessa lagar. I den situationen gäller de särskilda lagarnas bestämmelser om gallring med mera.

Lagen innehåller därutöver bestämmelser om bl.a. granskning och förstöring av uppgifter som i huvudsak motsvarar regleringen i rättegångsbalken. Vidare anges att SIN ska underrättas om ett beslut om inhämtning av uppgifter enligt denna lag.

Tillgång till abonnemangsuppgifter enligt lagen om elektronisk kommunikation

Av lagen om elektronisk kommunikation följer att de brottsbekämpande myndigheterna från en leverantör får begära uppgift om abonnemang, som det annars råder tystnadsplikt för, om uppgiften gäller misstanke om brott. Det krävs alltså inte något beslut från domstol, utan beslutet fattas av myndigheten. Med abonnemangsuppgifter avses framför allt uppgifter om namn, adress, IP-adress och abonnentnummer. Skyldigheten att lämna ut dessa uppgifter är numera inte begränsad till att gälla brott av viss svårighetsgrad.

Pejling

Det förekommer även att de brottsbekämpande myndigheterna inhämtar lokaliseringsuppgifter genom s.k. pejling. Denna metod innebär i korthet att myndigheten i hemlighet fäster en sändare på ett föremål, exempelvis ett fordon, en container eller en väska, och därefter följer föremålets rörelser med hjälp av radiopejling eller via satellit. För närvarande är sådana åtgärder inte reglerade på annat sätt än av den generella regleringen i 8 § polislagen.

18.5.3 Risker för den personliga integriteten

Det har i olika sammanhang konstaterats att tillgången till uppgifter om elektronisk kommunikation är av mycket stor betydelse i nästan all verksamhet som rör utredning av allvarlig brottslighet.[7] Uppgifterna anses ofta vara den viktigaste informationen för att föra utredningar om grova brott framåt. Det gäller särskilt i inledningsskedet av utredningsarbetet, då en kontroll av uppgifter som har genererats i anslutning till en brottsplats tillsammans med annan information kan göra det möjligt att komma vidare i utredningen. Uppgifter om elektronisk kommunikation används också i princip i varje utredning rörande grova brott som t.ex. mord, människorov, grovt rån, grov mordbrand, allmänfarlig ödeläggelse, grov våldtäkt,

[7] Beredningens för rättsväsendets utveckling delbetänkande, *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*, SOU 2005:38 s. 323 och departementspromemorian *Datalagring, EU-rätten och svensk rätt*, Ds 2014:23 s. 34 f. och 51 f.

människohandel för sexuella ändamål, grovt barnpornografibrott och grovt narkotikabrott samt brott som faller inom Säkerhetspolisens område.[8]

Tillgången till uppgifter om elektronisk kommunikation kan göra det möjligt att klarlägga såväl händelser som anknyter till själva brottstillfället som händelser som anknyter till planläggningen och flykten. Uppgifterna kan t.ex. leda till att en gärningsman kan identifieras, gömställen upptäckas, flyktbilar eller stöldgods påträffas och att bortförda personer eller döda kroppar kan hittas. När det gäller utredningar om viss internetrelaterad brottslighet, exempelvis barnpornografibrott och olika former av ärekränkningsbrott, är tillgången till uppgifter om elektronisk kommunikation ofta helt avgörande för att t.ex. kunna identifiera en misstänkt gärningsman.

En grundläggande förutsättning för att brottsbekämpande myndigheter ska kunna få ut denna typ av uppgifter från en tjänsteleverantör när ett brott har begåtts är att tjänsteleverantören fortfarande har uppgifterna i behåll, dvs. inte har raderat dem.

Samtidigt innebär såväl lagringen som utlämnandet av uppgifter ett stort intrång i enskildas personliga integritet. De lagrade uppgifterna är många gånger av sådan karaktär att de sammantaget ger möjlighet att dra mycket detaljerade slutsatser om enskildas privatliv, bl.a. om deras vanor i vardagslivet, dagliga förflyttningar och sociala relationer.

Den generella skyldigheten för bl.a. tele- och internetoperatörer att för brottsbekämpande ändamål lagra vissa uppgifter avseende samtliga abonnenter skiljer sig dessutom från övriga riktade åtgärder som presenterats i detta kapitel. Den här skyldigheten innebär en avvikelse från den väl etablerade dataskyddsprincipen att personuppgiftansvariga bara får lagra personuppgifter som de själva har ett behov av. Här är det i stället fråga om en skyldighet för operatörerna att samla in och spara uppgifterna för att vissa av dem eventuellt kan komma till nytta för de brottsutredande myndigheterna. För att en sådan generell skyldighet ska vara acceptabel förutsätts att nyttan är så stor, eller t.o.m. avgörande för att vissa brott över huvud taget ska vara möjliga att utreda, att skyddet för den personliga integriteten får stå tillbaka. I en sådan intresseavvägning ska, förutom graden av nytta och behov, även hänsyn tas till om uppgifternas innehåll har

[8] Ds 2014:23 s. 34.

begränsats så långt som möjligt, förutsättningarna och formerna för åtkomst, hur länge uppgifterna sparas samt den tekniska och administrativa informationssäkerheten. Dessa frågor har behandlats i tidigare utredningar[9] och lagstiftningen är för närvarande föremål för en översyn.[10] Kommittén finner det därför inte meningsfullt att i sin kartläggning fördjupa sig ytterligare i den här frågan, utan nöjer sig med att konstatera att lagringen av bl.a. trafikdata för brottsbekämpande ändamål är unik i ett principiellt hänseende.

När det gäller de brottsbekämpande myndigheternas tillgång till nu aktuella uppgifter kan konstateras att de kan få tillgång till abonnemangsuppgifter, som jämförelsevis är mindre känsliga från integritetssynpunkt, oavsett brottets svårighetsgrad och utan domstolsprövning. För tillgång till trafik- och lokaliseringsuppgifter under en förundersökning krävs däremot att det är fråga om relativt allvarlig brottslighet. Den prövningen inkluderar också ett förhållandevis stort antal rättssäkerhetsgarantier, bl.a. domstolsprövning och begränsningen av den krets som får granska uppgifterna. Det sistnämnda minskar risken för oönskad spridning av insamlade uppgifter. Det finns även bestämmelser om underrättelse i efterhand som framstår som väl avvägda samt den ovan nämnda tillsynen av användningen av hemliga tvångsmedel.

För att myndigheterna ska kunna få tillgång till trafik- och lokaliseringsuppgifter enligt inhämtningslagen inom ramen för underrättelseverksamhet, krävs att det är fråga om ännu allvarligare brottslighet. Samtidigt ger den lagen en möjlighet för myndigheterna att få tillgång till uppgifterna utan domstolsprövning. Uppgifter som har inhämtats på sådant sätt får inte användas i en förundersökning, om det inte också har meddelats ett tillstånd till hemlig övervakning av elektronisk kommunikation. Vid SIN:s granskning har det dock kunnat konstateras att det har förekommit att inhämtade uppgifter har använts i en förundersökning trots att det inte har förelegat något beslut om hemlig övervakning av elektronisk kommunikation.[11] SIN har även uppmärksammat att det har förekommit att polisen inhäm-

[9] Trafikuppgiftsutredningens betänkande *Lagring av trafikuppgifter för brottsbekämpning*, SOU 2007:76, Ds 2014:23 samt Datalagringsutredningens betänkande *Datalagring och integritet*, SOU 2015:31.

[10] Datalagringsutredningens slutbetänkande har remissbehandlats under sommaren 2015, dnr Ju2015/3153/Å.

[11] Säkerhets- och integritetsskyddsnämndens (SIN:s) uttalande den 11 september 2014, dnr 156-2014.

tat uppgifter enligt nämnda lag utan att informera SIN om åtgärden, vilket polisen är skyldig att göra[12]. Det har även konstaterats andra fel, t.ex. att uppgifter har hämtats in beträffande brottslighet som inte är sådana brott som kan ligga till grund för sådant inhämtande och att tillstånd om realtidsinhämtning har pågått längre än vad lagen föreskriver.[13]

Vidare har det förekommit att Säkerhetspolisen beslutat om inhämtning av uppgifter om elektronisk kommunikation trots att de faktiska omständigheterna inte rimligtvis kunnat föranleda en misstanke om sådan brottslig verksamhet för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Därtill avsåg beslutet dels inhämtning av uppgifter om meddelanden i realtid, dels inhämtning av lokaliseringsuppgifter under en period överstigande en månad från dagen för beslutet, vilket inte är tillåtet enligt inhämtningslagen. SIN ansåg att förhållandena i det sist aktuella fallet var så anmärkningsvärda att det var nödvändigt att göra en anmälan till Åklagarmyndigheten.[14]

Den särskilda utredare, som sett över lagringen av trafikdata för brottsbekämpande ändamål, har även haft i uppdrag att utvärdera inhämtningslagen samt att föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till bestämmelser om tillgång till och behandling av sådana uppgifter. Kommittén finner därför inte skäl att här göra någon fördjupad analys av frågan.

När det slutligen gäller pejling så anses det vara ett effektivt verktyg och viktigt komplement till exempelvis hemlig avlyssning av elektronisk kommunikation. Genom metoden är det utan risk för upptäckt möjligt att följa hur exempelvis någon i ett fordon som transporterar vapen, cigaretter, narkotika eller alkohol rör sig, för att kunna dra slutsatser om bl.a. rekognoseringar och var möten äger rum, mönster i körningar, klarläggande av avlämningsplatser och lagerplatser samt var medgärningsmän befinner sig.

Även pejling innebär dock ett beaktansvärt integritetsintrång, exempelvis när sändaren placeras på en personbil och därigenom gör det möjligt att kartlägga vilka platser som besöks med detta fordon. Det framstår därför som motiverat att komplettera det allmänna

[12] SIN:s uttalande den 13 februari 2014, dnr 162-2013, och den 27 mars 2014, dnr 14-2013.
[13] SIN:s uttalande den 9 oktober 2014, dnr 895-2014 och 896-2014.
[14] SIN:s uttalande den 16 oktober 2015, dnr 119-2015.

proportionalitetskravet som gäller enligt 8 § polislagen med ytterligare bestämmelser som stärker skyddet på den personliga integriteten vid denna typ av åtgärder.

Sammanfattningsvis innebär bl.a. lagringen av trafikuppgifter för brottsbekämpande ändamål, och viss tillgång till sådana uppgifter utan domstolsprövning, särskilda risker från integritetssynpunkt. Dessutom är användningen av sändare för pejling i princip oreglerad, trots att den innebär ett beaktansvärt integritetsintrång.

18.6 Genomsökning och kopiering av mobiltelefoner och datorer

18.6.1 Företeelsen

Det är inte ovanligt att polisen bereder sig tillgång till innehållet i mobiltelefoner och datorer för att inhämta uppgifter i brottsutredande syfte. Det förekommer även att hela innehållet i mobiltelefonen eller datorn kopieras.

18.6.2 Det skyddande regelverket

Befogenheterna för polisen att söka efter uppgifter som finns lagrade i datorer eller mobiltelefoner är inte underkastade någon specialreglering. En mobiltelefon eller en dator får liksom andra föremål som skäligen kan antas ha betydelse för utredning om brott tas i beslag enligt 27 kap. rättegångsbalken. Ett föremål som har tagits i beslag får undersökas och den information som föremålet innehåller vid beslagstillfället får tas ut, under förutsättning att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. Det anses däremot vara oklart om de brottsbekämpande myndigheterna får läsa ett meddelande, exempelvis ett sms, som mottas efter beslagstidpunkten.[15] Det krävs ett beslut om husrannsakan (28 kap. rättegångsbalken) för att bereda sig tillgång till en dator respektive en mobiltelefon om dessa inte är tillgänglig för beslag, t.ex. för att föremålet finns i en bostad.

[15] Åklagarmyndighetens beslagshandbok s. 34.

Trots att frågan inte uttryckligen reglerats anses de brottsbekämpande myndigheterna ha rätt att kopiera hela innehållet vid sin undersökning av beslagtagna mobiltelefoner och datorer, under förutsättning att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse.[16]

Vissa skriftliga handlingar, t.ex. meddelanden mellan en misstänkt och dennes försvarare, får dock inte tas i beslag. För vissa andra skriftliga handlingar, exempelvis meddelanden mellan den misstänkte och någon honom eller henne närstående, eller mellan sådana närstående inbördes, gäller att handlingen får tas i beslag endast om det är fråga om ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Det har dock framförts olika uppfattningar om dessa undantags räckvidd när det gäller elektroniska handlingar.[17]

Avsaknaden av särskild reglering innebär vidare att det inte finns något generellt förbud mot att använda överskottsinformation som erhållits vid kopiering av en mobiltelefon eller dator. Vissa allmänna bestämmelser, exempelvis polisdatalagen, sätter dock vissa gränser för behandlingen av sådana uppgifter och uppställer dessutom vissa krav när det gäller bl.a. gallring.

Förundersökningsutredningen har i sitt betänkande[18] föreslagit ett antal förtydliganden som tar sikte på just genomsökning och kopiering av innehållet i bl.a. mobiltelefoner och datorer. Förslaget innebär bl.a. att det införs uttryckliga bestämmelser om att beslagtagen egendom får kopieras och om att exempelvis en dator eller mobiltelefon som kan antas innehålla korrespondens mellan en misstänkt och dennes försvarare inte får genomsökas utan att den hos vilken beslaget gjorts och försvararen har beretts tillfälle att närvara vid undersökningen. Utredningen har även föreslagit att det inte ska vara tillåtet att ta ytterligare del av innehållet om det konstateras att datorn eller mobiltelefonen innehåller uppgifter som omfattas av tystnadsplikt. Även detta förslag har varit på remiss och bereds för närvarande i regeringskansliet.[19]

---

[16] Europeiska domstolens för de mänskliga rättigheterna dom i målet *Robathin mot Österrike* (30457/06).

[17] Utredningens om it-brottskonventionen betänkande *Europarådets konvention om it-relaterad brottslighet*, SOU 2013:39, s. 151.

[18] Förundersökningsutredningens betänkande *Förundersökning – objektivitet, beslag, dokumentation m.m.*, SOU 2011:45.

[19] Dnr Ju2011/4074/Å (arbete med lagrådsremiss pågår).

18.6.3 Risker för den personliga integriteten

Mobiltelefoner och datorer kan innehålla information om den misstänktes kontakter med andra som är av stor betydelse för brottsutredningen och som inte kan erhållas på annat sätt. Genom att hela innehållet kopieras säkerställs att det kan undersökas utan risk för att originalet ändras eller går förlorat. En kopiering av hela innehållet kan dessutom göra det möjligt att lämna tillbaka originalet tidigare än vad som annars vore fallet, och på så sätt i någon mening begränsa de negativa konsekvenserna för den misstänkte.

Samtidigt innehåller datorer och mobiltelefoner vanligtvis en hel del information som saknar betydelse för brottsutredningen, bl.a. känslig information av privat natur. Många mobiltelefoner fungerar i dag som små datorer. Genom att hela innehållet kopieras ökar risken för oönskad spridning av all den information som kan bäras av enheten.

Tömning av telefoner är dessutom ett mycket vanligt beslag. Det kan även nämnas att Datainspektionen vid en inspektion har konstaterat att en polismyndighet hade samlat en mycket stor mängd överskottsinformation från sådana s.k. mobiltömningar i en sökbar databas, utan att vid vare sig registrering eller gallring pröva uppgifters relevans för undersökningens ändamål såsom krävs enligt lag.[20]

En kopiering som följs av ett återlämnande av originalet anses dessutom medföra att den misstänkte förlorar möjligheten att påkalla rättens prövning av beslaget, vilket kan vara till nackdel för denne.

Av dessa skäl och då innebörden av gällande rätt är oklar i vissa avseenden, exempelvis när det gäller korrespondens mellan en misstänkt och dennes försvarare, finns av integritetsskäl ett behov av förtydliganden på detta område.

[20] Datainspektionens beslut den 26 april 2012, dnr 1849-2011.

18.7 Polismyndighetens informationsinhämtning på internet m.m.

18.7.1 Företeelsen

Behovet av spaning på internet ökar i takt med att allt mer kriminell verksamhet, t.ex. narkotikahandel, begås på internet. Viss information kan hämtas in genom att polisen endast tar del av befintlig information på internet, medan annan inhämtning görs genom att polisen är aktiv på internet. Information kan hämtas in öppet, utan att polisen i fråga döljer sin identitet, eller dolt, på så sätt att inhämtningen görs utan spårbarhet till polisen.

Polismyndigheten använder även internet, inklusive sociala medier, för att bl.a. få in tips och vittnesuppgifter, men även för att sprida information i syfte att öka tryggheten hos medborgarna samt för att minska brottsligheten och stärka förtroendet för Polismyndigheten. För att möjliggöra detta har polisen ett flertal Facebooksidor och Twitter-konton. Dessa konton administreras oftast lokalt, av exempelvis ett närpolisområde.

Polismyndigheten inhämtar också information från sociala medier och datorföretag som tillhandahåller e-posttjänster. Typiskt sett lämnar sådana aktörer ut abonnentuppgifter och IP-loggar, t.ex. information om från vilka IP-adresser som inloggningar gjorts på ett visst konto under en viss tidsperiod. När det gäller förfrågningar till vissa företag fungerar Nationella operativa avdelningen vid Polismyndigheten som s.k. Single Point of Contact för svensk polis, för att förfrågningarna ska vara likformiga och kvalitetssäkrade.

18.7.2 Det skyddande regelverket

I 8 § polislagen finns ett generellt krav på att en polisman som har att verkställa en tjänsteuppgift ska under iakttagande av vad som föreskrivs i lag eller annan författning ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Därutöver har den tidigare Rikspolisstyrelsen gett ut en handledning med rubriken *Polisen i sociala medier*[21], som uppdateras kontinuerligt. Handledningen behandlar bl.a. organisatoriska, juridiska och

[21] KA-159-3040/11.

etiska frågor och innehåller även konkreta råd och tips för polisens närvaro i sociala medier. När det gäller omnämnandet av personer i inlägg anges att information som kan riskera brottsoffers eller brottsmisstänktas integritet och säkerhet inte får publiceras. Inte heller får information som gör att läsaren kan identifiera en enskild individ läggas ut.

Eventuell insamling och efterföljande behandling av personuppgifter måste därutöver göras i enlighet med de generella krav för behandling av personuppgifter som följer av bl.a. polisdatalagen.

I princip alla sociala medier och datorföretag som tillhandahåller e-posttjänster har sitt säte utomlands. Deras utlämnande av uppgifter till svensk polis regleras därför av utländsk rätt. Vissa av aktörerna har därutöver egna regelverk och riktlinjer som kompletterar deras respektive nationella lagstiftning. I praktiken innebär detta att dessa aktörer i regel förser svensk polis med uppgifter om abonnenter och IP-loggar när det föreligger s.k. dubbel straffbarhet, dvs. när det brott som utreds i Sverige även är straffbart enligt aktörens nationella lagstiftning. Polismyndigheten måste alltså lämna information om vilken brottsrubricering ärendet gäller samt i regel även viss dokumentation, t.ex. skärmdumpar, angående det specifika brottet.

För att svensk polis ska få ut innehållet i exempelvis ett e-postmeddelande krävs däremot en begäran om internationell rättshjälp, dvs. att svenska myndigheter begär bistånd från exempelvis en åklagare eller domstol i den andra staten. Den svenska lagstiftningen om rättslig hjälp i brottmål finns huvudsakligen i lagen (2000:562) om internationell rättslig hjälp i brottmål. Vissa kompletterande bestämmelser återfinns dock i lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar.

18.7.3 Risker för den personliga integriteten

Polisens spaningsverksamhet på internet hör till ett område med svag reglering. Riskerna handlar t.ex. om bristande insyn över vilka uppgifter som samlas in och behandlas.

18.8 Tillgång till uppgifter i flygbolagens databaser (Passenger Name Record, PNR) och i EU:s informationssystem för viseringar (VIS)

18.8.1 Företeelsen

Flygbolagen samlar passageraruppgifter (Passenger Name Records, PNR) i sina databaser. Många av dessa uppgifter kommer från passagerarna själva (de har t.ex. lämnats vid bokning av en resa), medan andra uppgifter kommer från exempelvis resebyråer, hotell eller biluthyrare. Vissa av dessa uppgifter överförs på begäran till de brottsbekämpande myndigheterna. Vidare för Polismyndigheten ett register över passagerare som ankommer direkt från länder som varken ingår i EU eller Schengensamarbetet.

Inom EU har dessutom skapats ett gemensamt informationssystem för viseringar (VIS), vilket i första hand syftar till att förbättra genomförandet av den gemensamma viseringspolitiken. De brottsutredande myndigheterna inhämtar i viss utsträckning in uppgifter även från det systemet.

18.8.2 Det skyddande regelverket

Om uppgifterna kan antas ha betydelse för myndighetens brottsbekämpande verksamhet, får Tullverket respektive Polismyndigheten enligt 6 kap. 23 § tullagen (2000:1281) och 15 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska Unionen respektive 25 § polislagen kräva att exempelvis flygbolag lämnar ut PNR-uppgifter om passagerares namn, resväg, bagage, medpassagerare samt betalnings- och bokningssätt. Av nämnda bestämmelse i polislagen framgår vidare att även Säkerhetspolisen kan kräva ut PNR-uppgifter.

Av lagen (2006:444) om passagerarregister framgår vidare att Polismyndigheten, med hjälp av automatiserad behandling, ska föra ett register (passagerarregistret) över passagerare som ankommer direkt från länder som varken ingår i EU eller Schengensamarbetet. Syftet med registret är att underlätta verkställandet av personkontroller vid Sveriges gräns mot stater som varken tillhör Europeiska

unionen eller Schengenområdet. Personuppgifterna får i viss utsträckning lämnas ut till Säkerhetspolisen och Tullverket och ska i regel gallras inom 24 timmar efter överföringen till Polismyndigheten.

Med förbehåll för vissa särregler i lagen om passagerarregister, exempelvis nyss nämnda gallringsskyldighet, gäller att inhämtade uppgifter ska behandlas i enlighet med regleringen i lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet respektive polisdatalagen.

Genom Europeiska unionens råds beslut[22] skapade EU ett gemensamt informationssystem för viseringar (VIS). Ändamålet, funktionen och ansvarsfördelningen för VIS, inklusive villkoren för utbyte av uppgifter mellan medlemsstaterna, regleras i Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008. De brottsbekämpande myndigheternas tillgång till dessa uppgifter baseras på rådets beslut[23] och regleras i lagen (2000:343) om internationellt polisiärt samarbete och förordningen (2010:705) om internationellt polisiärt samarbete. Regleringen innebär i korthet att Polismyndigheten, för egen räkning eller på begäran av Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket eller Kustbevakningen, genom direktåtkomst får söka uppgifter i VIS, om det i enskilda fall finns skäl att anta att uppgifter i systemet väsentligen kan komma att bidra till att utreda viss allvarlig brottslighet, eller om det finns skäl att anta att uppgifter i systemet väsentligen kan komma att bidra till att förebygga, förhindra eller upptäcka sådan brottslighet. Det finns dock vissa begränsningar av vilka sökbegrepp som får användas. Vidare gäller att personuppgifter som har hämtats från VIS får behandlas för det ändamål som uppgifterna hämtades för samt för att utreda eller beivra brott i det enskilda fall som sökningen avsåg.

18.8.3 Risker för den personliga integriteten

Precis som vid annan insamling och efterföljande behandling av personuppgifter finns en risk att fler uppgifter än nödvändigt samlas in och används för andra ändamål än det för vilket de samlades in. Denna risk ökar om uppgifterna inte gallras på ett ändamålsenligt sätt.

[22] Rådets beslut 2004/512/EG av den 8 juni 2004.
[23] Rådets beslut 2008/633/RIF av den 23 juni 2008.

Kommissionen presenterade i februari 2011 ett förslag till direktiv om användning PNR-uppgifter för brottsbekämpande ändamål inom EU. Europaparlamentet röstade igenom förslaget den 15 april 2016. Direktivet ska reglera skyldigheten för flygbolag att överföra passageraruppgiftssamlingar till enheter för passagerarinformation i medlemsstaterna, för vilka ändamål uppgifterna får behandlas, hur länge uppgifterna får lagras och under vilka förutsättningar de får lämnas ut. Flygpassageraruppgifterna får endast behandlas för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

I mars 2016 tillsatte den svenska regeringen en utredare som ska föreslå hur direktivet om passageraruppgifter ska genomföras i Sverige.[24]

18.9 Polisens behandling av personuppgifter i register och databaser

18.9.1 Företeelsen

I polisens verksamhet behandlas en betydande mängd uppgifter, bl.a. i ett stort antal register av olika storlek och slag och med olika funktioner. Många uppgifter i dessa register, t.ex. uppgifter om att en person är misstänkt för brott, är känsliga ur integritetssynpunkt.

18.9.2 Det skyddande regelverket

Vid behandling av personuppgifter i Polismyndighetens och till stor del även Säkerhetspolisens brottsbekämpande verksamhet gäller polisdatalagen. Polisdatalagen gäller även för den polisiära verksamheten vid Ekobrottsmyndigheten samt vid behandling av personuppgifter i särskilda register i Nationellt forensiskt centrum (tidigare Statens kriminaltekniska laboratorium). Lagen gäller för automatiserad behandling av personuppgifter och för viss annan behandling av personuppgifter som ingår i en strukturerad samling av personuppgifter.

[24] Dir 2016:22.

Viss behandling av personuppgifter är undantagen från polisdatalagens tillämpningsområde och regleras i stället i andra författningar, nämligen lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister och lagen (2010:362) om polisens allmänna spaningsregister. Polisdatalagen gäller som huvudregel inte heller när personuppgifter behandlas i polisens vapenregister enligt vapenlagen (1996:67).

Inom ramen för sitt tillämpningsområde gäller polisdatalagen i stället för personuppgiftslagen, men lagen hänvisar till ett stort antal bestämmelser i personuppgiftslagen. För den personuppgiftsbehandling som inte avser brottsbekämpande verksamhet, exempelvis tillståndsgivning eller mer renodlad övervakning och ordningshållande verksamhet, är dock personuppgiftslagen direkt tillämplig.

I polisdatalagen anges för vilka ändamål personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Personuppgifter får behandlas om de behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra förpliktelser som följer av internationella åtaganden. Personuppgifter får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i framför allt brottsbekämpande verksamhet hos vissa andra myndigheter, däribland Säkerhetspolisen, Ekobrottsmyndigheten och Åklagarmyndigheten. I ett enskilt fall får personuppgifter behandlas genom att lämnas ut även för något annat ändamål än de som anges i lagen, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

För behandling av känsliga personuppgifter finns särskilda begränsningar. Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Det är alltså inte tillåtet att föra register över enskilda enbart på den grunden att de utifrån ras, etniskt ursprung eller något annat i paragrafen angivet förhållande kan hänföras till en viss kategori av människor. Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana personuppgifter när det är absolut nödvändigt för syftet med behandlingen. Det innebär att om andra uppgifter om en person samlas in i sam-

band med t.ex. en förundersökning får dessa kompletteras med uppgifter om t.ex. religiös övertygelse eller etniskt ursprung om det är av avgörande betydelse för utredningen.[25]

Känsliga personuppgifter kan förekomma i förundersökningar av många olika anledningar, t.ex. uppgifter om hälsa i olika undersökningar som görs eller på grund av att någon under ett förhör har lämnat en sådan uppgift eller i en inlaga nämnt uppgiften, bl.a. när det gäller vissa brottstyper såsom sexual- eller hatbrott. Om det nedtecknade förhöret eller den inkomna handlingen ingår i förundersökningen omfattas behandlingen av den känsliga personuppgiften även i dessa fall av undantaget.

När en uppgift inte längre behövs för något tillåtet ändamål ska den gallras, dvs. göras digitalt oåtkomlig. Det finns dessutom vissa generella tidsgränser för hur länge uppgifter får bevaras. Dessa tidsgränser innebär att uppgifterna i vart fall ska gallras efter ett, tre, fem eller tio år, beroende på vad uppgiften gäller.

Tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. För uppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet finns särskilda och mer begränsande regler till skydd för den personliga integriteten, t.ex. krav på markering när uppgifter avser en person som inte är misstänkt.

I polisdatalagen finns också särskilda bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Dessa bestämmelser reglerar bl.a. ändamålen för Säkerhetspolisens personuppgiftsbehandling, som delvis avviker från regleringen för den övriga polisen. Det finns även särskilda bestämmelser om bevarande och gallring.

Vissa register är föremål för särskild reglering i polisdatalagen, bl.a. DNA-registret, utredningsregistret och spårregistret som alla är register över DNA-profiler. DNA-registret innehåller DNA-profiler (information om identitet men inte om personliga egenskaper) avseende personer som har dömts till annan påföljd än böter, eller godkänt ett strafföreläggande som avser villkorlig dom, medan utredningsregistret innehåller motsvarande DNA-profiler avseende personer som är skäligen misstänkta för brott på vilket fängelse kan följa. I spårregistret finns däremot DNA-profiler som

[25] SIN:s uttalanden den 11 december 2014, dnr 67-2014 och 69-2014, om polismyndigheters behandling av känsliga personuppgifter i underrättelseverksamhet.

har tagits fram under utredning av brott och som inte kan hänföras till en identifierbar person. Även fingeravtrycks- och signalementsregistret, penningtvättsregistret samt det internationella registret omfattas av särskild reglering i polisdatalagen. Gemensamt för alla dessa register är att det finns särskilda bestämmelser om ändamål, gallring och direktåtkomst.

Vidare innehåller lagen (2014:400) om Polismyndighetens elimineringsdatabas särskilda bestämmelser om elimineringsdatabasen. Även det registret innehåller DNA-profiler, men inte från dömda eller misstänkta brottslingar utan från anställda vid Polismyndigheten och vissa andra som kan komma i kontakt med och därigenom riskerar att kontaminera exempelvis prover som ska bli föremål för DNA-analys. Uppgifterna i denna databas får endast behandlas för att upptäcka och utreda kontamineringar vid DNA-analyser och hanteringen av DNA-spår.

Ett register som däremot är av mer direkt betydelse för brottsbekämpningen är polisens allmänna spaningsregister (ASP). Registret regleras framför allt i lagen (2010:362) om polisens allmänna spaningsregister och förordningen (2010:1157) om polisens allmänna spaningsregister. Ändamålet med ASP är att underlätta tillgången till sådan information som behövs i polisens spaningsverksamhet. Personuppgifter som framkommit i polisens brottsbekämpande verksamhet får behandlas i ASP för detta ändamål. Registret används såväl i polisens utredningsverksamhet som i dess underrättelseverksamhet. Ekobrottsmyndigheten, Tullverket och Kustbevakningen har direktåtkomst till registret.

Det finns vissa begränsningar som gäller för att uppgifter om en misstänkt person ska få registreras i ASP. Det brott som avses och som den registrerade kan misstänkas för får inte endast ha böter i straffskalan. Vidare krävs att uppgiften är av särskild betydelse för polisens spaningsverksamhet. Uppgiften ska alltså kunna bidra till att brott av en tillräcklig svårighetsgrad kan beivras.[26] Det finns vidare särskilda krav för registrering av uppgifter om personer som inte är misstänkta för brott (s.k. kringpersoner). När det gäller sådana personer ska det bl.a. framgå att personen inte är misstänkt för brott.

[26] Prop. 2009/10:85 s. 289 och 376).

18.9.3 Risker för den personliga integriteten

Användning av modern informationsteknik i form av bl.a. olika typer av register är numera en naturlig del i så gott som allt polisiärt arbete och av stor betydelse för polisens möjligheter att kunna bedriva sin verksamhet på ett effektivt och rättssäkert sätt. Samtidigt måste detta arbete göras med respekt för enskildas integritet.

En stor del av de uppgifter som behandlas är av integritetskänslig karaktär. Ett exempel är naturligtvis uppgifter om att någon är misstänkt för brott, men även många andra känsliga uppgifter om t.ex. hälsa och sexualliv, religiös övertygelse, politiska åsikter och etniskt ursprung behandlas i stor utsträckning. Här kan också nämnas den betydande mängd genetiska data som förekommer i form av DNA-profiler i DNA-registren och som teoretiskt sett kan användas för att ta fram mycket detaljerad information om personer, även om användningsområdet i dag endast är att slå fast om spår från en brottsplats kommer från en viss person eller inte. Det behandlas också integritetskänsliga uppgifter om personer som inte är misstänkta för brott. När det gäller uppgifter om dessa personer är emellertid kraven ännu högre för att polisen ska få behandla dem.

När verksamheten i en så stor organisation som Polismyndigheten till stor del baseras på insamling och bearbetning av information finns risk att det skapas register vars användning är helt eller delvis otillåtna. Det kan exempelvis inträffa att det skapas register som överhuvudtaget inte får existera, eller som i vart fall innehåller otillåtna, felaktiga eller gamla uppgifter. Det kan även förekomma att tillgången till personuppgifter inte blir så begränsad för respektive tjänsteman som polisdatalagen förutsätter. Liknande risker kan även finnas i en mindre organisation som Ekobrottsmyndigheten. Erfarenheterna från senare tid visar att det fortfarande finns betydande problem när det gäller följsamheten till gällande reglerverk. Som exempel på detta kan nämnas följande.

Efter en omfattande granskning riktade Datainspektionen[27] kritik mot dåvarande Rikspolisstyrelsens behandling av personuppgifter i ASP. Av beslutet framgår bl.a. att registret innehöll uppgifter som enligt Datainspektionen saknade särskild betydelse för polisens spaningsverksamhet. Datainspektionen gjorde bedömningen att det pågick en inte obetydlig registrering av personuppgifter i ASP som

[27] Beslut den 21 mars 2014 (dnr 205-2013).

var olaglig. Bland de namn på grupperingar som förekommer i ASP påträffades dessutom vissa namn som innehåller känsliga personuppgifter, exempelvis ”rasister” och ”zigenare”, ”kringresande romer” och ”romer”. Eftersom känsliga personuppgifter inte får användas för sökningar i ASP innebär detta en risk för otillbörliga integritetsintrång. Datainspektionen framhöll också att ASP är extra integritetskänsligt, bl.a. på grund av att kraven för att registrera uppgifter i registret är låga och för att även personer som inte är misstänkta för brott får registreras. Datainspektionen ansåg även att det var av betydelse att det är många inom polisen som har tillgång till registret.[28]

Även Säkerhets- och integritetsskyddsnämnden har tidigare i samband med granskning av ASP konstaterat vissa brister, framför allt i fråga om rutiner för behandling av känsliga personuppgifter .[29]Datainspektionen har dessutom uppmärksammat att Nationellt forensiskt centrum tidigare gjort en otillåten jämförelse mellan DNA-profiler i laboratoriets elimineringsdatabas och det spårregister som förs med stöd av polisdatalagen.[30] Elimineringsdatabasen är numera lagreglerad.

Vidare har Säkerhets- och integritetsskyddsnämnden granskat Rikspolisstyrelsens behandling av personuppgifter i penningtvättsregistret (PTR) och framfört kritiken att det i flera granskade ärenden har saknats lagliga förutsättningar att behandla vissa personuppgifter. Det konstaterades också att gallring av personuppgifter i ett granskat ärende inte har gjorts i rätt tid samt att rutinerna var sådana att det fanns risk att motsvarande fel skulle begås igen.[31]

Säkerhets- och integritetsskyddsnämnden har även granskat Polismyndigheternas i Östergötland och Västra Götalands län behandling av personuppgifter i underrättelseverksamhet. Nämnden har sedan uttalat kritiken att känsliga personuppgifter i flera fall har behandlats utan att det har varit absolut nödvändigt, att uppgifter har varit tillgängliga i en alltför vid krets och att det närmare ändamålet med behandlingen av personuppgifter i vissa uppgiftssamlingar

[28] Polisen överklagade de delar av beslutet som gällde hur polisen gallrar uppgifter i registret och hanterar personer med skyddade personuppgifter. Förvaltningsrätten i Stockholm avslog överklagandet i dom den 18 mars 2015 (mål nr 8685-15) och Kammarrätten i Stockholm har beslutat att inte meddela prövningstillstånd (beslut den 29 september 2015 i mål nr 3435-15).

[29] Beslut den 22 januari 2013 (dnr 15-2013).

[30] Beslut den 28 maj 2012, dnr 514-2012).

[31] Uttalande den 13 februari 2014 bl.a. dnr 111-2013.

har varit alltför vitt. Nämnden påtalade också att uppgifter behandlats utan att det har funnits något konkret behov av dem, att det närmare ändamålet med behandlingen i vissa fall inte framgått tillräckligt tydligt, att det i vissa fall inte har framgått tillräckligt tydligt vilka personer som inte är misstänkta för brott samt att uppgifter inte har gallrats i rätt tid.[32]

Ett annat uppmärksammat exempel är Polismyndighetens i Skåne s.k. kringresanderegister som Säkerhets- och integritetsskyddsnämnden har kritiserat.[33] Av nämndens uttalande framgår bl.a. att polismyndighetens behandling av personuppgifter var olaglig i flera avseenden. Enligt nämnden var den allvarligaste bristen att ändamålet med personuppgiftsbehandlingen var alldeles för vitt och därför inte gav några ramar för personuppgiftsbehandlingen, att det inte fanns behov av att registrera alla de personer som fanns i uppgiftsamlingen, inte ens med det vida ändamål som gällt, och att det inte fanns ett tillräckligt tydligt samband mellan den av polismyndigheten angivna brottsligheten och de personuppgifter som behandlades. Sammantaget bedömdes uppgiftssamlingen därför i vart fall delvis ha fått karaktären av en ”bra att ha”-uppgiftssamling. Justitiekanslern gjorde sedermera bedömningen att bristerna sammantagna var så allvarliga att de personer vilkas uppgifter behandlats i nämnda register blivit utsatta för en sådan kränkning av den personliga integriteten som ger dem rätt till ersättning av staten enligt 48 § personuppgiftslagen.[34] Säkerhets- och integritetsskyddsnämnden har senare konstaterat att Polismyndigheten i Skåne har vidtagit åtgärder för att korrigera dessa felaktigheter[35]. Även Justitieombudsmannen[36] har konstaterat att det förelegat brister och uttalat kritik mot polisen och elva av de registrerade har vid Stockholms tingsrätt väckt en skadeståndstalan mot staten.[37]

Sedan det uppmärksammats att en polismyndighet hade fört ett register över misshandlade och hotade kvinnor som innehållit mycket känsliga uppgifter om kvinnorna och deras anhöriga, inledde Datainspektionen en granskning av nämnda register. Vid denna

[32] Uttalande den 11 december 2014 (dnr 67-2014 respektive 69-2014).
[33] Uttalande den 15 november 2013 (dnr 173-2013).
[34] Justitiekanslerns beslut den 7 maj 2014, dnr 1441-14-47.
[35] Dnr 463-2013.
[36] Beslut den 17 mars 2015, dnr 5205-2013.
[37] Tingsrättens mål nr T 2978-15, T 2986-15, T 2993-15, T 2996-15, T 2998-15, T 3002-15, T 3006-15, T 3010-15, T 3011-15, T 3012-15 och T 3013-15.

granskning konstaterade Datainspektionen bl.a. att registret var olagligt och bröt mot regler i såväl gamla och nya polisdatalagen som personuppgiftslagen. Registret innehöll bl.a. uppgifter av typen ”Lätt förståndshandikappad kille”, ”Psykopatvarning”, ”Borderline samt bipolär”, ”Mytoman” och ”Styvsonen homosexuell”. Registret innehöll dessutom tio år gamla registreringar. Inga uppgifter hade gallrats ur registret trots att polisen i alla sina register löpande ska pröva vilka uppgifter som ska finnas kvar. Datainspektionen konstaterade vidare att polisen själva för flera år sedan fattade beslut om att upphöra med det här registret, men att verksamheten ändå fortsatt som om inget har hänt samt att det tyder på bristande intern kontroll och uppföljning inom polisen. Datainspektionen har därför förelagt polisen att genast sluta använda registret.[38]

Vidare har Säkerhets- och integritetsskyddsnämnden anmält ett annat fall där polisen behandlat uppgifter om en person enbart på grund av dennes religiösa övertygelse och gjort bedömningen att detta kan utgöra brott.[39] Nämnden har även i en granskning granskat Polismyndighetens behandling av personuppgifter i polisens signalementsregister och funnit systematiska brister vad gäller gallring av uppgifter.[40] Mot den bakgrunden, och med beaktande av att det är system med mycket stor spridning, föranledde bristerna skarp kritik. Nämnden konstaterade även att drygt 27 000 användare har formell behörighet till systemet. Nämnden uppmanade därför Polismyndigheten att se över behörighetstilldelningen och rutinerna för att ompröva och avsluta tilldelade behörigheter i systemet.

Det har även förekommit att Polismyndigheten, i syfte att få allmänhetens hjälp att identifiera personer misstänkta för brott, har publicerat bilder från övervakningskameror på internet. Efter att klagomål mot ett sådant förfarande hade anmälts till Justitieombudsmannen, anförde Justitieombudsmannen bl.a. följande i sitt beslut:

> För att en sådan åtgärd ska vara rättsenlig och lämplig i övrigt, krävs att åtgärden är av synnerlig vikt för utredningen, att bilderna visar någon som utför vad som objektivt sett är ett brott eller försök till brott och att det för brottet inte ska vara föreskrivet lindrigare straff än fängelse i sex månader.

[38] Datainspektionens beslut den 24 juni 2015, dnr 2790-2014.
[39] Dnr 67-2014.
[40] SIN:s uttalande den 15 december 2015, dnr 2015-47.

> Om det rör sig om särskilt grov brottslighet eller om den misstänkte på goda grunder kan antas vara farlig för allmänheten eller enskilda, kan en publicering undantagsvis vara försvarbar även utan ett så starkt bevisläge.[41]

När det gäller s.k. kringpersoner, dvs. personer som inte själva är misstänkta för brott, har Datainspektionen dessutom vid en granskning av Tullverkets behandling av personuppgifter i dess brottsbekämpande verksamhet uppmärksammat brister när det gäller uppfyllandet av skyldigheten i 16 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet att förse registrerade uppgifter med en särskild upplysning om att personen i fråga inte är misstänkt för brott.[42]

Som nämns i avsnitt 18.6.3 har Datainspektionen dessutom vid inspektion av en s.k. särskild undersökning vid Polismyndighetens i Stockholms län kriminalunderrättelseverksamhet konstaterat bl.a. att Polismyndigheten framför allt genom s.k. mobiltömningar hade kommit över en mycket stor mängd överskottsinformation, bl.a. uppgifter om tidigare misstänktas kontaktnät, och registrerat bl.a. uppgifter från telefonernas adressböcker i en sökbar databas. Det konstaterades även att det beträffande 98 procent av dessa uppgifter, varken vid registrering eller senare gallring hade prövats om registreringen uppfyller lagens krav. Datainspektionen, som även noterade att ett flertal anställda hade tillgång till databasen och att det saknas spårbar behandlingshistorik som visar vad den inloggade har vidtagit för åtgärder, förelade därför Polismyndigheten i att upphöra med denna behandling av personuppgifter.[43]

Det har även i andra sammanhang uppmärksammats brister när det gäller polisens gallring av uppgifter.[44] Gallringsbestämmelserna syftar i första hand till att skydda den enskildes integritet genom att sätta en yttersta tidsgräns för det intrång som behandlingen innebär. Ett sätt att komma till rätta med dessa problem kan vara att förbättra det tekniska stödet så att systemet automatiskt raderar vissa uppgifter efter viss tid, eller i vart fall uppmärksammar användaren på

[41] Justitieombudsmannens beslut den 21 december 2010, dnr 4787-2009.
[42] Datainspektionens beslut den 12 juni 2014, dnr 111-2013.
[43] Datainspektionens beslut den 26 april 2012, dnr 1849-2011.
[44] Datainspektionens beslut den 21 mars 2014 (dnr 205-2013) samt SIN:s uttalanden den 13 februari 2014 (dnr 111-2013) och den 11 december 2014 (dnr 67-2014 och dnr 69-2014).

behovet av gallring. Detta försutsätter också att myndigheterna erhåller tillräckliga resurser för att bl.a. ta fram och utveckla sådant teknikstöd.

Det förekommer att tjänstemän vid Polismyndigheten döms för dataintrång som består i att de har använt polisregister för att ta fram uppgifter som de inte behövs i tjänsten, exempelvis gjort slagningar på sig själva eller sina närstående. Under de senaste åren har dock myndigheten i viss utsträckning stramat upp sina rutiner för att undvika den typen av beteende, bl.a. genom olika varningstexter på dataskärmen och s.k. loggning av sökningar i vissa register, dvs. att sökhistorik sparas så att det i efterhand går att se vem som gjort vad. Denna uppstramning bör leda till att antalet dataintrång inom polisen minskar. Förekomsten av dataintrång som begås av anställda visar dock på behovet av att också begränsa den faktiska tillgången till uppgifter som inte är nödvändig för t.ex. olika personalkategorier. Utformningen och tilldelningen av behörigheter är ett viktigt verktyg för att uppnå det integritetsskydd som föreskrivs i polisdatalagen, liksom intern kontroll, genom t.ex. loggning, och uppföljning.

Det kan skada allmänhetens förtroende för de brottsbekämpande myndigheternas verksamhet att reglerna fortfarande inte följs fullt ut. Omorganisationen av polisen innebär en möjlighet för verksamheten att ta krafttag för att komma till rätta med de problem med att följa bestämmelserna som framgår av nämnda uttalanden och beslut från tillsynsmyndigheterna.

Enligt uppgift som framförts från Polismyndigheten till kommittén har myndigheten på senare tid genomfört ett flertal åtgärder som är ägnade att stärka skyddet för den personliga interiteten. Det handlar bl.a. om skärpta rutiner för behörighetstilldelning, ökad spårbarhet och förbättrad åtkomstkontroll.

18.10 Internationellt informationsutbyte

18.10.1 Företeelsen

Sverige har genom olika internationella överenskommelser åtagit sig att överlämna information som härrör från brottsbekämpande verksamhet dels till polis- och åklagarmyndigheter i andra länder, dels till

organisationer som Interpol[45] och Europol[46]. På samma sätt erhåller de svenska brottsbekämpande myndigheterna information från utländska myndigheter. Uppgifter delas både inom underrättelseverksamheten och inom ramen för förundersökning, och kan omfatta uppgifter om såväl särskilda organisationer och företeelser som enskilda individer.

Informationsutbytet görs i olika situationer. En situation är när Sverige har förbundit sig att tillhandahålla information av visst slag utan särskild begäran, genom direktåtkomst eller på annat sätt. Det kan också vara fråga om att Sverige i en överenskommelse har åtagit sig att genomföra en viss åtgärd eller lämna viss information på begäran av en annan stat eller mellanstatlig organisation. Uppgiftsutlämnandet kan också vara spontant på initiativ av den svenska polisen.

18.10.2 Det skyddande regelverket

De uppgifter som utländska myndigheter önskar att få del av omfattas många gånger av sekretessbestämmelser i offentlighets- och sekretesslagen (2009:400), framför allt bestämmelser om sekretess till skydd för den brottsbekämpande verksamheten och till skydd för enskilda vilkas uppgifter behandlas i sådan verksamhet, men även andra sekretessbestämmelser kan vara aktuella. Enligt lagen får utlämnande av uppgifterna får dock ändå göras till en utländsk myndighet om utlämnandet görs i enlighet med särskild föreskrift i lag eller förordning. Sådana föreskrifter finns i polisdatalagen och innebär att personuppgifter får lämnas ut till Interpol, Europol, eller en polismyndighet eller åklagarmyndighet som är ansluten till Interpol i vissa brottsbekämpande syften, om det är förenligt med svenska intressen. Detsamma gäller utlämnande till utländsk underrättelse- eller säkerhetstjänst. Uppgifter får vidare lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Bestämmelsen tar framför allt sikte på utlämnande av uppgifter till Europol.

[45] En mellanstatlig polisorganisation där medlemsstaterna i arbetet mot gränsöverskridande brottslighet samarbetar inom ramen för respektive medlemslands nationella lagstiftning.

[46] Europeiska polisbyrån, ett av EU:s brottsbekämpande organ som samordnar utbytet av underrättelseinformation mellan medlemsstaterna framför allt när det gäller grov gränsöverskridande brottslighet.

Enligt offentlighet- och sekretesslagen får utlämnande också göras om uppgiften i motsvarande fall skulle få lämnas till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas ut. Ett exempel på sådant utlämnande är när en svensk myndighet i samband med en begäran om rättslig hjälp i en förundersökning lämnar ut sekretessbelagda uppgifter till en utländsk myndighet i syfte att få ett visst förhör genomfört.

Av polisdatalagens hänvisning till vissa bestämmelser i personuppgiftslagen följer ett förbud mot att föra över personuppgifter till ett land som inte är medlem i EU eller anslutet till EES (ett s.k. tredjeland), om landet inte har en adekvat nivå för skyddet av personuppgifterna. Från denna regel gäller dock vissa undantag. Här kan även nämnas kravet på uppgifter som samlats in för ett visst ändamål, inte får lämnas ut om utlämnandet är oförenligt med det ursprungliga ändamålet, vilket när det gäller detta område i normalfallet torde vara att förhindra och bekämpa brott.

I många fall kan uppgifter lämnas ut med villkor som begränsar mottagarens användning av uppgiften. Det kan t.ex. handla om att begränsa mottagarens möjlighet att lämna uppgiften vidare eller på annat sätt använda den. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige och i vissa fall inte heller innehålla andra begränsningar än sådana som får föreskrivas vid överföring inom Sverige.

Det finns därutöver ett antal författningar som reglerar utlämnandet av personuppgifter till utländska myndigheter i vissa särskilda situationer, däribland följande.

- I *lagen (2000:343) om internationellt polisiärt samarbete* regleras samarbete mellan svenska brottsbekämpande myndigheter och motsvarande myndigheter i andra medlemsstater i EU samt Norge och Island. Lagen reglerar bl.a. Schengensamarbetet och Prüm-samarbetet (som ger polismyndigheter inom EU rätt att söka i varandras DNA-, fingeravtrycks- och fordonsregister), men även annat samarbete som är konventionsbundet. Informationsutbyte inom ramen för Schengensamarbetet regleras dock framför allt i *lagen (2000:344) om Schengens informationssystem.*

- *Lagen (2003.1174) om vissa former av internationellt samarbete i brottsutredningar* innehåller regler om gränsöverskridande samarbete i enskilda brottsutredningar.
- *Lagen (2000:1219) om internationellt tullsamarbete* reglerar det internationella tullsamarbete som syftar till att förhindra, upptäcka, utreda och beivra överträdelser av tullbestämmelser.
- *I lagen (2000:562) om internationell rättslig hjälp* regleras skyldigheten för svensk myndighet att på en utländsk myndighets begäran vidta vissa åtgärder, som exempelvis hemliga tvångsmedel. En sådan begäran handläggs i Sverige av domstol eller åklagare, som kan begära biträde av bl.a. Polismyndigheten. I princip används samma tillvägagångssätt som vid motsvarande svensk åtgärd. Lagen innehåller också bestämmelser om i vilken utsträckning svenska myndigheter kan begära rättslig hjälp utomlands.

Genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen infördes kompletterande bestämmelser för genomförde av rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (det s.k. dataskyddsrambeslutet). Lagen innehåller regler som gäller för viss behandling av personuppgifter vid det gränsöverskridande samarbetet mellan de brottsbekämpande myndigheterna inom EU samt Island, Norge, Schweiz och Liechtenstein.

18.10.3 Risker för den personliga integriteten

Det internationella utbytet av information spelar en viktig roll för bekämpningen av framför allt allvarlig och gränsöverskridande brottslighet.[47] Det finns dock en risk för att informationsutbytet leder till en förlorad kontroll över flödet av personuppgifter och för att den nationella lagstiftningen inte kan säkerställa ett skydd för informationen. Informationen kan t.ex. komma att användas för andra syften eller få en större spridning än vad som varit avsett. Det kan vidare vara svårt att åstadkomma rättelse och utplåning m.m. avse-

[47] Se bl.a. prop. 2009/10:85 s. 170.

ende uppgifter som har överförts till andra länder. Det måste också beaktas att graden av känslighet hos personuppgifter kan variera mellan olika länder. Vidare kan det, som bl.a. Säkerhets- och integritetsskyddsnämnden konstaterat i en rapport[48], innebära praktiska svårigheter för en myndighet att bedöma om den mottagande staten vid ett s.k. tredjelandsutlämnande har en adekvat nivå för skyddet av personuppgifter. De risker som ett utlämnande av information kan medföra innebär att stora krav måste ställas på att bestämmelserna följs och på möjligheterna till kontroll av detta. En förutsättning för att extern granskning ska kunna genomföras och vara effektiv är naturligtvis att skälen för fattade beslut dokumenteras.[49]

18.11 Kommitténs samlade bedömning av området

De brottsbekämpande myndigheterna inhämtar information om enskilda på en rad olika sätt och ofta information som är känslig från integritetssynpunkt. Mycket av informationen behandlas därefter bl.a. i olika register. Åtgärderna motiveras av intressen att förebygga, utreda eller beivra brott. Dessa intressen måste anses vara legitima och centrala i en rättsstat. Dessutom syftar brottsbekämpningen i många fall till att skydda just enskildas personliga integritet i olika avseenden.

I detta kapitel om brottsbekämpande verksamhet har kommittén behandlat risker för integritetsintrång i samband med dessa företeelser:

- Hemliga tvångsmedel med stöd av 27 kap. rättegångsbalken (hemlig rumsavlyssning, hemlig kameraövervakning, hemlig avlyssning och övervakning av elektronisk kommunikation samt genomsökning och kopiering av mobiler och datorer).
- Användning av spaningsmetoder som främst regleras av polislagen.
- Polisens aktivitet på internet.
- Behandling av personuppgifter i register
- Tillgång till uppgifter i flygbolagens register.

[48] SIN:s rapport den 9 juni 2011, dnr 886-2010.
[49] Jfr ovan nämnda rapport samt SIN:s uttalande den 22 maj 2013, dnr 205-2012.

- Internationellt informationsutbyte.

Behovet av, nyttan med och risken för integritetsintrång på grund av olika tvångsmedel har varit föremål för en omfattande kartläggning, framför allt inom ramen för Utredningen om vissa hemliga tvångsmedel.[50] Utredningen gjorde dels en totalundersökning där man inhämtade uppgifter från de brottsbekämpande myndigheterna om varje enskilt ärende där den aktuella lagstiftningen tillämpats, dels djupundersökningar av vissa ärenden. Av kartläggningen framgår bl.a. att det överlag finns ett stort behov av tvångsmedlen samt att vissa tvångsmedel anses vara av särskild nytta, men att det framför allt i utredningar om organiserad brottslighet är av avgörande betydelse att information kan inhämtas på många olika sätt. Samtidigt konstaterades att tvångsmedlen medför integritetsintrång, som dock såväl de brottsbekämpande myndigheterna som domstolarna på olika sätt försökt begränsa vid den praktiska tillämpningen. Det har alltså gjorts en grundlig genomgång där intresset av en effektiv brottsbekämpning har vägts mot intresset av skydd för den enskildes personliga integritet.

Under de senaste åren har det dock mer eller mindre kontinuerligt pågått en rad olika och delvis överlappande lagstiftningsprojekt på området. Så är fallet även i dag. Dessa ständigt pågående förändringar av regelverket gör det svårt att bedöma den samlade effekten av åtgärderna från ett integritetsperspektiv. Samtidigt har vissa lagändringar under senare tid inneburit att regleringen i ökande grad har samlats i 27 kap. rättegångsbalken[51] och därmed gjorts mer överblickbart, vilket får anses vara positivt även ur ett integritetsperspektiv. Vidare har i större utsträckning uppställts krav på beslut från domstol för användning av tvångsmedlen. För dessa ärenden hos domstol har också införts ett ökat krav på offentliga ombud som ska bevaka enskildas integritetsintressen.

[50] SOU 2012:44.
[51] Prop. 2011/12:55 och prop. 2013/14:237.

Hemliga tvångsmedel med stöd av 27 kap. rättegångsbalken

Tvångsmedlen som utförs med stöd av 27 kap. rättegångsbalken är alltså väl reglerade och innefattar olika skyddsfunktioner för den personliga integriteten. När det gäller hur gällande regelverk följs har dock Säkerhets- och integritetsskyddsnämnden i sin tillsynsverksamhet uppmärksammat att även om de brottsbekämpande myndigheterna hanterar hemliga tvångsmedel på ett i huvudsak tillfredsställande sätt, föreligger vissa brister i verksamheten. En brist som uppmärksammats är att det material (upptagningar eller uppteckningar) som erhållits genom hemlig tvångsmedelanvändning i vissa fall inte har förstörts tillräckligt snabbt.[52] Det har vidare konstaterats brister bl.a. i myndigheters dokumentation som inneburit att det inte alltid varit möjligt att följa handläggningen av tvångsmedelsärendena samt att hantering av underrättelser till enskilda i flera avseenden varit undermålig.[53]

Kommittén bedömer ur ett riskperspektiv att det föreligger viss risk för den personliga integriteten i samband med användning av olika tvångsmedel med stöd av 27 kap. rättegångsbalken. Vid denna bedömning har kommittén beaktat sannolikheten för att gemene man ska träffas av åtgärden, liksom att företeelserna är väl reglerade och att risken för oönskad spridning är låg.

Ett hemligt tvångsmedel innebär dock ett mycket närgånget intrång i den personliga integriteten för den enskilda person som är föremål för åtgärden.

När det gäller den generella skyldigheten för teleoperatörer att lagra vissa trafikuppgifter gör kommittén bedömningen att denna företeelse utgör ett väsentligt avsteg från den väl etablerade principen att personuppgiftsansvariga bara får lagra personuppgifter som de själva har ett behov av.

Användning av spaningsmetoder som främst regleras av polislagen.

Det finns även ett antal företeelser som är av beaktansvärd betydelse från integritetssynpunkt men som trots detta är mer eller mindre oreglerade i dag, bl.a. användningen av dolda kroppsmikrofoner och

[52] Se t.ex. redovisning den 23 maj 2012 (dnr 97-2012) den 22 maj 2013, dnr 96-2013] respektive den 22 maj 2014 (dnr 891-2014).

[53] Se t.ex. SIN:s uttalanden den 25 mars 2015, dnr 137-2014 och 2088-2014).

handmanövrerade kameror samt möjligheterna att kopiera hela innehållet i datorer och mobiltelefoner. Dessa spaningsmetoder regleras i dag främst av 8 § polislagen. När det gäller dessa företeelser gör kommittén bedömningen att användningen av dessa metoder generellt sett är förknippade med påtaglig risk för intrång i den personliga integriteten.

Polisens spaningsverksamhet på internet och utåtriktade verksamhet i sociala medier

Denna företeelse hör också till ett område med svag reglering.[54] Riskerna handlar t.ex. om bristande insyn över vilka uppgifter som samlas in och behandlas. Kommittén gör bedömningen att dessa företeelser är förknippade med vissa risker för den personliga integriteten.

Behandling av personuppgifter i register

Även när det gäller Polismyndighetens behandling av personuppgifter i register har bl.a. Säkerhets- och integritetsskyddsnämnden uppmärksammat brister. Nuvarande brister förefaller handla om att gällande bestämmelser inte följs snarare än om utformningen av lagstiftningen som sådan. I det avseendet konstaterar kommittén att det finns utrymme för förbättringar. Den stora organisation som Polismyndigheten utgör innebär att en ännu större mängd uppgifter samlas hos en och samma myndighet samt att fler personer kan få tillgång till dessa uppgifter. Det ökar behovet av åtgärder för att säkerställa att uppgifter inte sprids till obehöriga personer i och utanför organisationen. När det gäller polisens behandling av personuppgifter i register bedömer kommittén att företeelsen är förknippade med påtagliga risker för intrång i den personliga integriteten.

Tillgång till uppgifter i flygbolagens register.

Vissa uppgifter från flygbolagen överförs på begäran till de brottsbekämpande myndigheterna. Vidare för Polismyndigheten ett register över passagerare som ankommer direkt från länder som varken ingår

[54] Se även kapitel 11 om E-förvaltning.

i EU eller Schengensamarbetet. Polisen hämtar i viss utsträckning in uppgifter även från EU:s gemensamma system för viseringar. Denna behandling av uppgifter om resenärer är förknippade med risk för att fler uppgifter än nödvändigt samlas in och även med en risk för att de används för andra ändamål än det för vilket de samlades in. Denna risk ökar om uppgifterna inte gallras på ett ändamålsenligt sätt. Det rör sig här om uppgifter om en stor mängd människor som reser och som inte ägnar sig åt brottslig verksamhet. Företeelsen är dessutom internationell. Det finns dock ett skyddande regelverk. Kommittén gör bedömningen att denna företeelse är förknippade med en viss risk för intrång i den personliga integriteten.

Internationellt informationsutbyte.

Polisens deltar även i annat internationellt samarbete om utbyte av uppgifter i brottsbekämpande verksamhet. Vid informationsutbyte finns risk för att det leder till en förlorad kontroll över flödet av personuppgifter och att den nationella lagstiftningen inte kan säkerställa ett skydd för informationen. Informationen kan t.ex. komma att användas för andra syften eller få en större spridning än vad som varit avsett. Det kan vidare vara svårt att åstadkomma rättelse och utplåning m.m. avseende uppgifter som har överförts till andra länder. Kommittén bedömer att denna företeelse är förknippad med en viss risk för intrång i den personliga integriteten.

Kommitténs övriga synpunkter

Utöver vikten av intern uppföljning bör också framhållas betydelsen av en effektiv och ändamålsenlig tillsyn. När det gäller den frågan har regeringen tillsatt en särskild utredning – Utredningen om en myndighet med ett samlat ansvar för tillsyn över den personliga integriteten – som har i uppdrag att bl.a. överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet. Uppdraget ska redovisas i september 2016.[55]

[55] Dir. 2014:164 och dir. 2015:139.

Ett annat problem är att myndigheterna i vissa fall inte uppfyller de krav som följer av ny lagstiftning på grund av att det föreligger tekniska problem på it-området. Som exempel på detta kan nämnas att bl.a. 10–11 §§ i gamla polisdatalagen aldrig fick genomslag på grund av att polisens it-system inte hade de funktioner som krävdes för att kunna uppfylla lagens bestämmelser. Motsvarande reglering finns i 3 kap. 10–13 §§ i nya polisdatalagen. Men dessa bestämmelser behöver inte börja tillämpas förrän den 1 januari 2018.

Avslutningsvis kan konstateras att när det gäller det brottsbekämpande arbetet har den enskilde, av naturliga skäl, begränsade möjligheter att bestämma vilken information som myndigheterna får behandla. Systemet med underrättelse om användningen av hemliga tvångsmedel i efterhand kan i viss mån anses väga upp denna brist. På så sätt får den enskilde åtminstone möjlighet att bedöma vilket integritetsintrång som förekommit och möjlighet att reagera mot sådant som han eller hon anser vara rättsstridigt. Det finns dock undantag från skyldigheten att underrätta den enskilde. I dessa fall finns däremot krav på att det i stället är Säkerhets- och integritetsskyddsnämnden som ska underrättas och som också ska underrättas vid inhämtning av uppgifter om elektronisk kommunikation enligt den s.k. inhämtningslagen. Nämnden ska även på begäran av enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel eller har varit föremål för polisens personuppgiftsbehandling. Nämnden ska även kontrollera om tvångsmedelsanvändningen och personuppgiftsbehandlingen har genomförts i enlighet med lag eller annan författning. Dessutom finns möjligheten för en registrerad att få ersättning för den skada eller kränkning av den personliga integriteten som en personuppgiftsbehandling i strid med lagen har orsakat.

19 Försvarsunderrättelseverksamhet och militär säkerhetstjänst

Kommitténs bedömning: Riskerna för den personliga integriteten i samband med signalspaning bedöms som påtagliga.

Det föreligger en viss risk för den personliga integriteten i samband med behandling av personuppgifter i den militära underrättelsetjänstens it-system.

Båda dessa företeelser innebär dock omfattande intrång i den personliga integriteten för dem som faktiskt blir föremål för dem.

19.1 Inledning

19.1.1 Allmänt om verksamheten

Försvarsunderrättelseverksamhet bedrivs för att identifiera, bevaka och bedöma yttre hot mot Sverige och svenska intressen i utlandet, till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Verksamheten går i korthet ut på att hämta in information som avser utländska förhållanden, vilken därefter bearbetas, analyseras och rapporteras som underrättelser till berörda myndigheter. Syftet är att ge en förvarning om utvecklingen i omvärlden, så att uppdragsgivarna inte överraskas.

Den militära säkerhetstjänsten syftar till att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och dess intressen i Sverige och utomlands. I arbetet ingår bl.a. att kartlägga och motverka främmande underrättelseverksamhet och annan säkerhetshotande verksamhet mot Försvarsmakten och dess säkerhetsintressen samt att identifiera och prioritera skyddsvärda tillgångar och

bedöma säkerhetshot. Vidare ingår att med tekniska åtgärder försöka förhindra obehörig insyn i och påverkan av telekommunikations- och it-system.

Militära underrättelse- och säkerhetstjänsten (Must), vid Försvarsmakten, ansvarar för den militära säkerhetstjänsten och bedriver även försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamhet bedrivs också av Försvarets radioanstalt (FRA), Totalförsvarets forskningsinstitut (FOI) och Försvarets materielverk (FMV). Vidare har FRA även i uppdrag att hjälpa samhällsviktiga verksamheter att skydda sin it-miljö.

Från integritetssynpunkt är det framför allt Must:s och FRA:s inhämtning och efterföljande behandling av personuppgifter som är av betydelse.

19.1.2 Den rättsliga regleringen

Personuppgiftsbehandlingen regleras framför allt i

- personuppgiftslagen (1998:204),
- lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst,
- förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst,
- lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet,
- förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet,
- lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen), samt
- förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet.

19.1.3 Tillsyn m.m.

Statens inspektion för försvarsunderrättelseverksamheten (Siun) är en nämndmyndighet under regeringen, som har till uppgift att kontrollera försvarsunderrättelseverksamheten så att den bedrivs i enlighet med lagar och förordningar. Siun är också kontrollmyndighet för den verksamhet som bedrivs signalspaningslagen. I kontrollen av signalspaningen ska Siun särskilt granska sökbegrepp, förstöring och rapportering. Vidare ska Siun på enskilds begäran kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning och, om så är fallet, ifall inhämtningen och behandlingen av inhämtade uppgifter har gjorts i enlighet med signalspaningslagen. Siun har också mandat att avbryta inhämtning eller besluta om förstöring av upptagning eller uppteckning, om det skulle visa sig att inhämtningen inte varit förenlig med det tillstånd som meddelats av Försvarsunderrättelsedomstolen.

Om Siun uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten eller annan behörig myndighet. Om nämnden uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person, ska nämnden anmäla det till Justitiekanslern. Om nämnden finner omständigheter som Datainspektionen bör uppmärksammas på, ska nämnden anmäla det till inspektionen.

Vidare är Datainspektionen tillsynsmyndighet för personuppgiftsbehandlingen vid bl.a. Försvarsmakten och FRA, enligt personuppgiftslagen respektive lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Post- och telestyrelsen har ett samlat tillsynsansvar inom området för elektronisk kommunikation. I uppdraget ingår bl.a. att utöva tillsyn över operatörernas överföring av signaler till samverkanspunkter från vilka FRA kan ta del av resultatet av signalspaningen.

Vid FRA finns även ett integritetsskyddsråd som har i uppgift att fortlöpande utöva insyn i de åtgärder som vidtas, för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådets ledamöter utses av regeringen.

I de fall uppgifter behandlas hos Polismyndigheten och Säkerhetspolisen efter att ha inhämtats med hjälp av signalspaning, har även Säkerhets- och integritetsskyddsnämnden ett tillsynsansvar.

Slutligen utövar Riksdagens ombudsmän (Justitieombudsmannen) och Justitiekanslern viss tillsyn över bl.a. Försvarsmaktens och FRA:s verksamheter.

19.2 Försvarets radioanstalts behandling av uppgifter i försvarsunderrättelseverksamhet (signalspaning)

19.2.1 Företeelsen

FRA bedriver signalspaning mot specifik internationell kommunikation, för att ge regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen vid Polismyndigheten unik information om viktiga utländska förhållanden.[1] FRA har alltså inte något eget försvarsunderrättelsebehov, utöver den verksamhet som bedrivs i syfte att utveckla de egna metoderna, utan signalspaning utförs på uppdrag av nämnda myndigheter.

Verksamheten bedrivs från stationer på olika platser i Sverige samt från flygplan och fartyg. Spaningen riktas mot såväl civila som militära radiosignaler som t.ex. telefoni och dataöverföring samt viss kabeltrafik som passerar rikets gräns. Den riktas även mot signaler som inte innehåller personuppgifter, t.ex. signaler från radar-, navigerings- och vapenrelaterade system.

Information (exempelvis trafikuppgifter eller uppgifter om innehållet i vissa telefonsamtal, sms eller e-postmeddelanden) hämtas in genom att sökbegrepp appliceras på signaler.

Sökbegreppen är utformade så att de väljer bort respektive väljer ut signaler som är av intresse för försvarsunderrättelseverksamheten. Inhämtade elektroniska signaler bearbetas och analyseras, varefter en rapport lämnas till uppdragsgivaren. Vissa underrättelser delges även andra berörda myndigheter.

[1] Säkerhetspolisens och Polismyndighetens möjlighet att inrikta signalspaning motiveras av deras behov av uppgifter om utländska förhållanden på strategisk nivå avseende bl.a. internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen.

Det förekommer även visst internationellt informationsutbyte. Utlämnande av uppgifter till andra länder kan för Försvarsmaktens och FRA:s del behöva göras inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Utlandssamarbete är också en del av verksamheten för den militära säkerhetstjänsten.

19.2.2 Det skyddande regelverket

FRA bedrev tidigare signalspaning i etern med stöd av principen att etern är fri. Denna princip, som bl.a. framgår av lagen (2003:389) om elektronisk kommunikation, har ansetts innebära att avlyssning i etern är fri, oavsett om den bedrivs av enskilda eller myndigheter. Principen om eterns frihet har dock blivit allt mer ifrågasatt, bl.a. med hänvisning till Europadomstolens praxis.[2]

Sedan den 1 januari 2009 regleras FRA:s möjlighet till signalspaning i signalspaningslagen. Lagen ger FRA möjlighet att även bedriva signalspaning i kabel. Den 1 december 2009 kompletterades lagen med vissa bestämmelser som stärkte skyddet för den personliga integriteten.[3] Ändringarna gällde bl.a. för vilka syften som inhämtning får göras samt att den ska vara föremål för domstolsprövning och utökad tillsyn.

Signalspaning i försvarsunderrättelseverksamhet får endast avse utländska förhållanden och utföras i syfte att kartlägga vissa angivna företeelser, bl.a. yttre militära hot mot landet, strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen samt främmande underrättelseverksamhet mot svenska intressen. Den närmare inriktningen av signalspaningen bestäms av uppdragsgivaren, dvs. regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen eller Nationella operativa avdelningen vid Polismyndigheten.

Tillstånd för signalspaning lämnas av Försvarsunderrättelsedomstolen efter ansökan av FRA. Ett tillstånd får ges för högst sex månader i taget. I tillståndet ska anges bl.a. vilka sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen samt de villkor i övrigt som behövs för att begränsa intrånget i enskildas personliga integritet.

---

[2] Polismetodutredningens betänkande *Särskilda spaningsmetoder*, SOU 2010:103 s. 74.
[3] Regeringens proposition *Förstärkt integritetsskydd vid signalspaning*, prop. 2008/09:201.

Inhämtning av signaler ska ske automatiserat med hjälp av sökbegrepp. En inriktning av signalspaningen får inte avse endast en viss fysisk person. Däremot får sökbegrepp som är direkt hänförliga till en viss fysisk person användas om det är av synnerlig vikt för verksamheten. När sådana sökbegrepp har använts ska personen underrättas om detta, om det inte hindras av sekretess eller inhämtningen uteslutande avser främmande makts förhållanden eller förhållanden mellan främmande makter.

Inhämtning får, som tidigare nämnts, göras i såväl etern som i kabel. Inhämtning av uppgifter i kabel får endast avse signaler som förs över Sveriges gräns i kabel som ägs av en operatör. Den får inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Detsamma gäller bl.a. om innehållet berör en fysisk person och detta har bedömts sakna betydelse för försvarsunderrättelseverksamheten samt vissa uppgifter som omfattas av tystnadsplikt enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Vidare innehåller lagen om behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet generella bestämmelser om behandling av personuppgifter hos FRA. Där framgår bl.a. att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål samt att uppgifterna inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Vidare framgår att i försvarsunderrättelseverksamheten får uppgifter om en person behandlas endast om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

I lagen finns dessutom särskilda begränsningar när det gäller bl.a. behandling av känsliga personuppgifter, t.ex. uppgifter om etniskt ursprung, politiska åsikter, religiös övertygelse eller hälsa. Sådana uppgifter får behandlas endast när det är absolut nödvändigt för syftet med behandlingen. Därutöver innehåller lagen bestämmelser om bl.a. personuppgiftsombud, säkerhet vid behandlingen, information till enskilda om ifall deras personuppgifter behandlas (när uppgifterna inte omfattas av sekretess) samt skadestånds- och straffansvar i vissa fall. Slutligen finns bestämmelser om gallring, som innebär att

personuppgifter som behandlas automatiserat ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas, om inte regeringen eller Riksarkivet har meddelat föreskrifter eller beslutat om annat.

Uppgifter hos FRA omfattas i stor utsträckning av sekretess (15 och 38 kap. offentlighets- och sekretesslagen [2009:400]).

Samarbete med andra länder får förekomma om syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. Vidare får uppgifter – även sekretessbelagda uppgifter – lämnas ut till en utländsk myndighet eller en internationell organisation, om utlämnandet tjänar den svenska statsledningen eller det svenska totalförsvaret. Ett utlämnande får inte göras om det är till skada för svenska intressen.

19.2.3 Risker för den personliga integriteten

Allmänna överväganden

Signalspaning anses vara av stor betydelse för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Metoden har under lång tid använts för att inhämta signaler i etern, men har först på senare tid reglerats i lag. Regleringen har inneburit bl.a. ökad kontroll av verksamheten, samtidigt som möjligheten att bedriva signalspaning även i kabel har medfört att FRA och dess uppdragsgivare fått tillgång till en betydligt större mängd uppgifter.

Personer som är involverade i de utländska företeelser som är av intresse för försvarsunderrättelseverksamhet, är i regel beroende av att kunna kommunicera via etern eller i kabel. Signalspaning anses vara en effektiv försvarsunderrättelsemetod för att snabbt få information om olika utländska företeelser. Tillsammans med annan underrättelseverksamhet kan signalspaning ge en samlad bild av en händelseutveckling som berör svensk utrikes-, säkerhets- och försvarspolitik. FRA följer delar av den utländska och internationella signaltrafiken och skapar sig därigenom en bild av normalläget. En avvikelse från normalbilden kan utgöra en varning om ett hot som föranleder någon form av åtgärd från uppdragsgivaren.[4]

[4] Signalspaningskommitténs betänkande *Uppföljning av signalspaningslagen*, SOU 2011:13 s. 31.

Vid signalspaning överförs all gränsöverskridande trafik i kabel till vissa samverkanspunkter, men det lagras inte uppgifter vid dessa punkter. Endast en mycket begränsad trafikmängd förs vidare till FRA via signalbärare. Trots detta innebär den verksamhet som bedrivs vid FRA att det i stor utsträckning inhämtas och bearbetas personuppgifter som kan vara av känslig natur. Genom signalspaning kan inhämtas uppgifter om vad enskilda talar om i telefon eller vad som skrivs i e-postmeddelanden. Det ligger i sakens natur att en stor del av det som sägs eller skrivs i denna trafik inte har att göra med de omständigheter som legat till grund för inhämtningen. I stället kan samtalen eller korrespondensen gälla t.ex. personliga förhållanden som helt saknar betydelse för försvarsunderrättelseverksamheten. Signalspaning innebär därför ett betydande intrång i den personliga integriteten, framför allt sedan spaningen utvidgats till att omfatta trafik i kabel. Utvidgandet av signalspaningen har bl.a. inneburit att den riktar sig mot en mycket stor mängd information.

Utformningen av sökbegrepp och den automatiska databehandling som informationsflödena möjliggör innebär visserligen att endast en ytterst liten del av den inhämtade informationen kommer under mänskliga ögon. Redan det faktum att staten bereder sig tillgång till informationen innebär dock ett integritetsintrång, även om intrånget blir större när ett visst meddelande avskiljs för analys genom sökbegreppen och informationen behandlas vidare.[5] Tillvägagångssättet kan också påverka enskildas upplevelse av att få sin privata sfär inskränkt och integritetsfrågan berör därför personer bosatta i Sverige i allmänhet.[6]

Det kan i detta sammanhang nämnas att det för närvarande pågår ett mål mot Sverige vid Europadomstolen, där det i korthet görs gällande att FRA:s signalspaning innebar en kränkning av rätten till privatliv såväl när frågan var oreglerad som efter ikraftträdandet av signalspaningslagen samt att signalspaningen även efter lagändringarna i december 2009 kränker rätten till privatliv.[7]

[5] *Polisens tillgång till signalspaning i försvarsunderrättelseverksamhet*, Ds 2011:44 s. 42 f. och Regeringens proposition *En anpassad försvarsunderrättelseverksamhet*, prop. 2006/07:63 s. 88.
[6] SOU 2011:13 s. 15.
[7] Ansökan nr 35252/08, *Centrum för rättvisa ./. Sverige.*

Resultat av granskning och kontroll

På regeringens uppdrag[8] genomförde Datainspektionen under år 2009 och 2010 en granskning av den personuppgiftsbehandling som tillämpningen av signalspaningslagen föranledde. Uppdraget var ett led i uppföljningen av lagen och innebar att Datainspektionen skulle analysera vilka särskilda integritetsproblem som kan uppstå i samband med personuppgiftsbehandling i FRA:s signalspaningsverksamhet. Datainspektionen skulle vidare utreda om de rutiner och riktlinjer som FRA tillämpar är tillräckliga för att hantera sådana problem samt bistå FRA vid utarbetandet av de ytterligare rutiner som kunde vara nödvändiga för att tillgodose integritetsskyddsbehovet.

Uppdraget redovisades i en rapport den 6 december 2010.[9] Den sammanfattande bedömningen var att frågor som har med personuppgiftsbehandling och personlig integritet att göra togs på allvar vid FRA samt att myndigheten lagt ned mycket tid och resurser på att skapa rutiner och utbilda personalen på ett sådant sätt att risken för otillbörliga intrång i den personliga integriteten minimeras. I sin rapport pekade Datainspektionen dock också på ett antal särskilda integritetsproblem som kan uppstå i verksamheten. En sådan faktor var den ökande trafikmängden i signalbärarna som möjligheten till kabelinhämtning kunde förväntas innebära. Som angavs i rapporten är trafiken i kabel mer uppblandad än vad som tidigare var fallet med den militära eterburna trafiken, som då också lättare kunde hållas åtskild från ”vanliga” människors kommunikation. Dagens tekniska lösningar innebär att personer med anknytning till de yttre hoten mot Sverige – t.ex. terrorverksamhet – i princip kommunicerar i samma nät som alla andra, vilket ställer högre krav på att FRA kan välja ut just de signaler som är relevanta för de utrikes förhållanden och yttre hot som FRA har till uppgift att rapportera. Att sådana signaler som inte är relevanta för verksamheten kan sållas bort är av stor vikt för att minimera intrånget i den personliga integriteten.

I sin rapport underströk Datainspektionen vidare att det vid granskningen inte gjorts några fynd som gav stöd för att det vid FRA pågått en omfattande personuppgiftsbehandling för syften som inte låg inom ramen för försvarsunderrättelseverksamheten såsom den

[8] Fö2009/355/SUND.

[9] *Rapport, Datainspektionens redovisning av regeringsuppdraget Fö2009/355/SUND.*

kommit till uttryck i lagstiftningen. Datainspektionen anförde att man således inte funnit att FRA behandlat uppgifter i syfte att förse de brottsbekämpande myndigheterna med information om t.ex. olaglig fildelning av upphovsrättsligt skyddat material eller liknande verksamhet. Datainspektionen gjorde inte heller några iakttagelser som tydde på att FRA behandlade personuppgifter i syfte att i största allmänhet kunna kartlägga internetanvändning, utan fann att den personuppgiftsbehandling som bedrevs gjordes för de syften som riksdag och regering bestämt.

När det gäller de särskilda integritetsproblem som kan uppstå i samband med signalspaningen pekade Datainspektionen bl.a. på att FRA borde överväga åtgärder som tekniska sökbegränsningar i databasen för trafikdata samt logguppföljning, i syfte att skydda personuppgifter mot otillbörliga intrång. Datainspektionen uppmärksammade även att FRA i stor omfattning använde sökbegrepp som var direkt hänförliga till en viss person, trots att sådana sökbegrepp endast får användas om det är av synnerlig vikt för utredningen. Vidare framhölls vikten av fungerande rutiner för att skilja bort uppgifter om s.k. inhemsk trafik samt att irrelevant information förstörs på ett sådant sätt att den inte kan återskapas, liksom att det måste finnas rutiner som säkerställer att sådana uppgifter behandlas endast när det är nödvändigt.

Även Signalspaningskommittén fick i uppdrag att följa signalspaningen vid FRA i syfte att utifrån rättsliga och etiska aspekter redovisa och bedöma vad FRA:s inhämtning av signaler har för konsekvenser för den enskildes integritet. I sitt betänkande[10] framhöll kommittén bl.a. att FRA har skapat rutiner som är avsedda att minimera otillbörliga intrång i enskildas personliga integritet samt att FRA tillämpar signalspaningslagen med försiktighet, utan att tänja på gränsen för det tillåtna. Vidare anfördes att en effektiv signalspaningsprocess strävar efter att begränsa underlaget till det som ur ett verksamhetsperspektiv utgör relevant information. FRA har därför intresse av att begränsa det inhämtade materialet till en hanterbar mängd information. Kommittén konstaterade att detta ligger inbyggt i verksamheten och gagnar integritetsskyddet. Kommittén gjorde

[10] SOU 2011:13.

vidare bedömningen att FRA har rutiner och regelverk som syftar till att förhindra att uppgifter som lämnas ut till andra länder skadar svenska intressen samt att integritetsintresset beaktas.

Kommittén anmärkte däremot, liksom Datainspektionen i nämnda rapport, att den underrättelseskyldighet som följer av signalspaningslagen i praktiken är verkningslös som skydd för enskildas integritet, på grund av den starka sekretess som vanligtvis gäller för uppgifter inom försvarsunderrättelseverksamheten. Kommittén framhöll i stället att den efterhandskontroll som Siun utför på begäran av enskild utgör ett viktigare instrument, eftersom denna innebär en granskningsmöjlighet från ett fristående och självständigt organ.[11]

Siun har sedan 2010 genomfört 10–15 granskningar per år av FRA. Därutöver har genomförts kontroller på enskildas begäran, avseende om den enskildes meddelanden har inhämtats vid signalspaning. Under 2014 genomfördes tio sådana kontroller (2012 och 2013 genomfördes fyra respektive 62 kontroller på enskildas begäran). Dessa granskningar har resulterat i ett fåtal synpunkter till FRA, bl.a. en synpunkt under 2014. Under perioden till och med 2014 uppmärksammade Siun inte någon brist som föranledde någon annan åtgärd, exempelvis att avbryta inhämtning eller rapportera frågan till regeringen eller annan myndighet.[12] Den 18 mars 2015 gjorde dock Siun en anmälan till Datainspektionen om att FRA tolkat en bestämmelse i signalspaningslagen på ett sätt som kan ifrågasättas.[13]Siuns kontrollverksamhet har i sin tur granskats av Riksrevisionen. I sin rapport[14] redovisar Riksrevisionen slutsatsen att Siun har fått förutsättningar att utföra sin granskning på ett effektivt sätt samt att Siun utför de uppgifter som myndigheten har enligt lagar och förordningar. Vidare anges att försvarsunderrättelsemyndigheterna tar Siuns synpunkter på allvar och genomför åtgärder i enlighet med Siuns beslut.

[11] SOU 2011:13, s. 77f.
[12] Siuns årsredovisningar 2009–2014).
[13] Siuns dnr 47-2014H:4.
[14] Kontrollen av försvarsunderrättelseverksamheten, RIR 2015:2.

Avslutningsvis kan noteras att Europarådets Venedigkommission, som består av experter i statsrätt, nyligen har studerat den demokratiska kontrollen av signalspaningen i Europarådets medlemsstater och i sin rapport lyft fram tillsynen i Sverige som ett gott exempel.[15]

19.3 Försvarsmaktens informationshantering i försvarsunderrättelseverksamhet- och militär säkerhetstjänst

19.3.1 Företeelsen

Must inhämtar information genom bl.a. fysisk spaning, informatörer och utländska samarbetspartners samt med tekniska hjälpmedel, framför allt den signalspaning som bedrivs av FRA. På så sätt får Must tillgång till omfattande information om enskilda personer. Informationen kan i vissa fall vara mycket integritetskänslig. Must behandlar därefter den insamlade informationen på olika sätt, bl.a. i sökbara register.

19.3.2 Det skyddande regelverket

Lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst innehåller bestämmelser om behandling av personuppgifter i nämnda verksamheter.

I lagen finns vissa grundläggande krav som överensstämmer med regleringen i personuppgiftslagen, t.ex. bestämmelser om att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål samt att uppgifterna inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.

När det gäller försvarsunderrättelseverksamhet får uppgifter om en person behandlas endast om uppgiften har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

[15] *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session, Venice, 20–21 March 2015 (CDL-AD[2015]006).*

Inom ramen för militär säkerhetstjänst får uppgifter om en person behandlas för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att 1) klarlägga verksamhet som innefattar hot mot rikets säkerhet, eller 2) vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet. Därutöver krävs i regel att

1. uppgifterna ger grundad anledning att anta att personen har begått eller kan komma att begå viss allvarlig brottslighet,
2. personen har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet, eller
3. uppgifterna avser information som har framkommit i samband med att en person har genomgått registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen (1996:627).

När det gäller den militära säkerhetstjänsten uppställs vidare krav på att uppgifter om en person ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas samt att det i förekommande fall ska framgå att personen inte är misstänkt för brottslig eller säkerhetshotande verksamhet. Uppgifter om att någon har begått eller kan komma att begå brott ska även förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Vidare gäller särskilda begränsningar bl.a. i fråga om behandling av känsliga personuppgifter, t.ex. uppgifter om etniskt ursprung, politiska åsikter, religiös övertygelse eller hälsa. Sådana uppgifter får behandlas endast när det är absolut nödvändigt för syftet med behandlingen.

Därutöver innehåller lagen bestämmelser om bl.a. personuppgiftsombud, säkerhet vid behandlingen, underrättelse om behandling (när uppgifterna inte omfattas av sekretess) samt skadestånds- och straffansvar i vissa fall. Slutligen finns bestämmelser om gallring, som bl.a. innebär att personuppgifter som behandlas automatiserat ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas, om inte regeringen eller Riksarkivet har meddelat föreskrifter eller beslutat om annat.

19.3.3 Risker för den personliga integriteten

För att Must ska kunna genomföra sitt uppdrag på ett effektivt sätt måste myndigheten samla in och behandla en stor mängd information. Denna information gäller i viss utsträckning enskilda personer och kan vara integritetskänslig. Det är därför av stor vikt att Must i vart fall inte behandlar fler uppgifter än vad som verkligen behövs och att behandlingen görs i överensstämmelse med gällande regelverk, exempelvis när det gäller gallring.

Datainspektionen genomförde under år 2012 och 2013 en granskning av den personuppgiftsbehandling som Must bedriver. Granskningen avsåg bl.a. personuppgiftsbehandling i it-systemen: IS UNDSÄK, OSINET och Säkerhetsregistret. Vidare lämnade Must viss information om bl.a. rutiner och arbetssätt.

Datainspektionens bedömning var att Musts generella arbete på personuppgiftsområdet var genomtänkt och följde en klar struktur, men att det fanns vissa brister. En sådan brist var att det fanns en risk att framför allt it-systemet IS UNDSÄK innehöll fler uppgifter än vad Must hade rätt att behandla. Ett skäl till detta var att promemorior och liknande lades in i systemet i oförändrat skick, till och med när de hade skrivits av någon utanför Must, utan att det gjordes någon bedömning av om alla uppgifter fick behandlas i systemet. Det saknades även rutiner för gallring och det var inte ens möjligt att utföra någon gallring i systemet. Vidare uppmärksammades att det i såväl IS UNDSÄK som Säkerhetsregistret hade registrerats personuppgifter utan att den rättsliga grunden angavs. Datainspektionen förelade därför Must att vidta åtgärder i dessa avseenden och påpekade dessutom att Försvarsmakten bör ta fram skriftliga rutiner eller föreskrifter för personuppgiftsbehandlingen i systemen.[16]

Efter Datainspektionens beslut har Försvarsmakten vidtagit en rad åtgärder för att möta dessa krav. Bland annat har en ny försvarsmaktsintern författning beslutats, nya rutiner för personuppgiftsbehandling fastställts, utbildning genomförts och en särskild referens- och granskningsgrupp organiserats.[17]

[16] Datainspektionens beslut 2013-03-28, dnr 1486-2012.
[17] Se bl.a. Datainspektionens skrivelse den 12 november 2013, dnr 1666-2013 samt Musts Årsöversikt 2014, s. 29.

Datainspektionens granskning illustrerar dock de risker för den personliga integriteten som föreligger vid behandling av stora mängder personuppgifter.

19.4 Kommittén samlade bedömning av området

Kommittén har i detta kapitel främst behandlat risker för intrång i den personliga integriteten vid behandling av personuppgifter vid signalspaning och vid behandling av personuppgifter i den militära underrättelsetjänstens it-system.

Inhämtningen av uppgifter i försvarsunderrättelseverksamhet och militär säkerhetstjänst syftar till att skydda Sverige och svenska intressen mot yttre hot, vilket är ett angeläget intresse. Säkerställandet av nationella säkerhetsintressen får i sig anses vara ett sådant ändamål som kan motivera inskränkningar av enskildas fri- och rättigheter. Att landet har en egen säkerhetpolitisk underrättelsesförmåga är också en förutsättning för att vi inte ska vara beroende av andra länders säkerhetsorgan.

Underrättelser hämtas in på en rad olika sätt, men signalspaningen är en av de grundläggande metoderna. Den tekniska utvecklingen på senare tid har inneburit att viktig information som tidigare kunde infångas genom signalspaning i etern, numera i allt högre utsträckning infångas via kabel.[18] Det finns mot den bakgrunden ett starkt intresse av att signalspaning även kan utföras i kabel, särskilt eftersom det saknas alternativa metoder för att uppnå motsvarande resultat.

Försvarsunderrättelsemyndigheterna hanterar dock en mycket stor mängd uppgifter, som många gånger är av privat natur. Det görs dessutom i en verksamhet som omgärdas av stark sekretess vilket innebär mycket begränsade möjligheter till insyn för allmänheten. Myndigheterna har också långtgående befogenheter i sin verksamhet. Detta innebär risker ur ett integritetsperspektiv, men kan i längden även få betydelse när det gäller medborgarnas tilltro till myndig-

[18] I 11:e septemberutredningens betänkande *Vår beredskap efter den 11 september, SOU 2003:32* s. 129, angavs att 98 procent av trafik till och från Sverige då gick genom kabel, enligt vad FRA upplyst.

heternas verksamhet. Mycket av den oro som framförts beträffande signalspaning har också handlat om bristande insyn och risken för missbruk.

Den enskilde har av naturliga skäl mycket begränsad insyn i och få möjligheter att påverka om och hur uppgifter behandlas i underrättelseverksamheten. Det finns visserligen en skyldighet för FRA att lämna underrättelser till enskild när det använts sökbegrepp som är direkt hänförliga till en viss fysisk person. Med hänsyn till den sekretess som personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten normalt sett omfattas av, måste dock denna skyldighet anses sakna en praktisk funktion som skydd för enskildas integritet.

När allmänhetens möjligheter till insyn är begränsade, är det desto viktigare med framför allt externa kontrollfunktioner. En viktig sådan funktion när det gäller signalspaningen är till att börja med den tillståndsprövning som görs av en självständig domstol och där en behovs- och proportionalitetsprövning ska göras. I den bedömningen ligger en prövning ur ett integritetsskyddsperspektiv.

Det finns också ett särskilt stort behov av effektiv efterhandsgranskning genom extern tillsyn. Utifrån vad som redovisas i nämnda rapporter och redovisningar från Siun och Datainspektionen framstår det som att de tillämpande myndigheterna tar integritetsfrågan på stort allvar och att följsamheten till gällande regelverk är god, även om vissa brister har uppmärksammats. Riksrevisionen har också bedömt att Siuns granskningsverksamhet i sin tur är effektiv och att försvarsunderrättelsemyndigheterna tar nämndens synpunkter på allvar och genomför åtgärder i enlighet med Siuns beslut.

Vid signalspaning överförs all gränsöverskridande trafik i kabel till vissa samverkanspunkter, men det lagras inga uppgifter vid dessa punkter och endast en begränsad trafikmängd förs vidare till FRA via s.k. signalbärare. Trots detta innebär den verksamhet som bedrivs vid FRA att det i stor utsträckning inhämtas och bearbetas personuppgifter som kan vara av mycket privat och känslig natur. Mot bakgrund av att uppgifterna hämtas in och behandlas av myndigheter som omgärdas av stark sekretess och stora befogenheter skulle kunna göras gällande att riskerna för den personliga integriteten i samband med signalspaning ska bedömas som allvarliga. Intrånget i den personliga integriteten är tveklöst mycket omfattande för de enskilda personer som faktiskt blir föremål för granskning. Mot bak-

grund av att det finns tydliga regler om på vilket sätt denna spaning får bedrivas, att kontrollfunktionerna förefaller att fungera och att endast en ytterst liten del av den totala informationen blir granskad, gör kommittén ändå den sammanvägda bedömningen att riskerna inom det här området ska betraktas som påtagliga.

När det gäller behandling av personuppgifter i Must:s it-system handlar det också om behandling av en stor mängd personuppgifter i en verksamhet med liten insyn. Intrånget i den personliga integriteten är tveklöst mycket omfattande för de enskilda personer vars personuppgifter behandlas. Kommittén bedömer dock att det är låg sannolikhet för gemene man att utsättas för denna risk. Kommittén bedömer även att det handlar om en begränsad spridning av de personuppgifter som behandlas. Kommittén bedömer därför att det föreligger en viss risk för intrång i den personliga integriteten i samband med denna typ av personuppgiftsbehandling.

Ovanstående bedömningar bygger på det underlag som kommittén har haft tillgång till.

Avslutningsvis ska nämnas att vissa utländska myndigheter samlar in och bearbetar information om Sverige och om personer som är bosatta i Sverige, på samma sätt som svenska myndigheter gör detta beträffande utländska förhållanden. Denna utländska verksamhet kan även ha andra syften, exempelvis att kartlägga egna medborgare som har flytt till Sverige (s.k. flyktingspionage). De utländska myndigheterna samlar in uppgifter bl.a. genom signalspaning, utan hänsyn till de begränsningar som gäller enligt svensk lagstiftning.

I vissa fall kan sådan utländsk verksamhet upplevas som mer integritetskränkande än om en svensk myndighet skulle ha agerat på motsvarande sätt, exempelvis om den utländska myndigheten arbetar åt en diktatur. I andra fall kan utländska myndigheters behandling av uppgifter upplevas som mindre integritetskränkande än motsvarande nationella behandling, t.ex. på grund av att den enskilde typiskt sätt inte behöver konfronteras med uppgifter som finns hos utländska myndigheter. Oavsett vilket är det uppenbart att även sådan utländsk verksamhet utgör en betydande risk för den personliga integriteten i Sverige. Det är dock svårt för kommittén att närmare bedöma hur och i vilken omfattning sådana intrång förekommer.

20 Övervakning med kamera

Kommitténs bedömning: Kameraövervakning innebär påtagliga risker för den personliga integriteten.

Lagring och vidarebearbetning av uppgifter som har samlats in med hjälp av kameraövervakning är förknippade med allvarliga risker för den personliga integriteten.

20.1 Inledning

20.1.1 Allmänt om kameraövervakning m.m.

I det här kapitlet behandlas personövervakning genom användning av TV-kameror och därmed jämförbar utrustning. De brottsbekämpande myndigheternas övervakning av enskilda, inom ramen för spanings- och utredningsarbetet, behandlas i kapitel 18. Vidare behandlas vissa frågor om kameraövervakning i skolor och i arbetslivet i kapitel 7 och 8.

Myndigheter och näringsidkare använder sedan många år tillbaka övervakningskameror för att förebygga, avslöja eller utreda brott. Sådana kameror förekommer bl.a. i bank-, post- och butikslokaler. Det är också förhållandevis vanligt att övervakningskameror används för att förhindra olyckor, exempelvis i tunnelbana eller fabriker.

Kameraövervakningen utfördes tidigare genom att video- och ibland även ljudsignaler skickades via tråd i ett slutet system från fasta kameror till ett kontrollrum, där mediaströmmen spelades in på band eller övervakades i realtid av personal som satt vid en eller flera TV-skärmar. Med teknikutvecklingen har förutsättningarna för kameraövervakning förändrats markant. Det är numera möjligt att ta mycket bra bilder på stora avstånd och färre kameror behövs för att

täcka in ett större område. Bild och ljud överförs ofta trådlöst via exempelvis internet. Dessutom kan stora datamängder lagras förhållandevis billigt på hårddiskar eller andra media. Det har också utvecklats små och billiga IP-baserade kameror (dvs. kameror som kan anslutas till internet med hjälp av internetprotokollet) som finns att köpa på konsumentmarknaden, vilket har medfört att även privatpersoner övervakar omgivningen med kamera. Digitaliseringen har dessutom skapat förutsättningar för en automatisk bildanalys, där datorer kan ta del av innehållet i en bildström och analysera detta innehåll samt i nästa steg fatta beslut baserat på vad som händer framför kameran.

20.1.2 Den rättsliga regleringen

Inledning

Personuppgiftslagen (1998:204), som gäller vid behandling av personuppgifter som helt eller delvis är automatiserad, innehåller generella bestämmelser om behandling av personuppgifter. Där finns bestämmelser som reglerar bl.a. när personuppgifter får behandlas samt krav på säkerhet och gallring vid behandling av personuppgifter. Lagen är dock subsidiär i förhållande till annan lagstiftning. Om det i annan lag eller författning finns bestämmelser som avviker från personuppgiftslagen gäller alltså denna andra reglering.

När det gäller kameraövervakning finns särskilda bestämmelser i kameraövervakningslagen (2013:460). Inom ramen för sitt tillämpningsområde gäller alltså den lagen i stället för personuppgiftslagen. Regleringen i kameraövervakningslagen beskrivs nedan.

Det bör dock nämnas att det även finns generella straffbestämmelser i brottsbalken som är av betydelse i detta sammanhang och som gäller oavsett om personuppgiftslagen eller kameraövervakningslagen är tillämplig. Det tydligaste exemplet på detta är att den som olovligen med tekniskt hjälpmedel i hemlighet tar upp bild av någon som befinner sig inomhus i en bostad eller på en toalett, i ett omklädningsrum eller ett annat liknande utrymme, kan dömas för kränkande fotografering till böter eller fängelse i högst två år (4 kap. 6 a § brottsbalken). Den som olovligen medelst tekniskt hjälpmedel för återgivning av ljud i hemlighet avlyssnar eller upptager tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller

annan sammankomst, vartill allmänheten icke äger tillträde och som han själv icke deltager i eller som han obehörigen berett sig tillträde till, kan även dömas för olovlig avlyssning till böter eller fängelse i högst två år (4 kap. 10 § brottsbalken). Under vissa förutsättningar kan även straffansvar för ofredande aktualiseras (4 kap. 7 § brottsbalken).

Kameraövervakningslagens syfte och tillämpningsområde

Kameraövervakningslagens syfte är att tillgodose behovet av kameraövervakning för berättigade ändamål, samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten. I kameraövervakningsförordningen (2013:463) finns kompletterande regler om bl.a. tillsyn.

Kameraövervakningslagen gäller endast kameraövervakning med TV-kameror, eller därmed jämförbar utrustning, som är uppsatta så att de, utan att manövreras på platsen, kan användas för personövervakning samt behandling av bild- och ljudmaterial som tagits upp vid sådan övervakning. Från lagens tillämpningsområde är kameraövervakning av plats dit allmänheten inte har tillträde undantagen, om övervakningen bedrivs av en fysisk person som ett led i verksamhet av rent privat natur. Det innebär att lagen normalt sett inte gäller för sådan övervakning i privatbostäder som utförs av den som bor där, likaså när det gäller t.ex. garage, förråd och på tomtmark. Det är dock inte fråga om privat kameraövervakning om bilder eller ljud från övervakningen är avsedda att spridas till en större krets personer.[1] När kameraövervakningslagen inte är tillämplig gäller, som tidigare nämnts, personuppgiftslagen på vanligt sätt.

Kameraövervakningslagen gäller inte heller vid s.k. hemlig kameraövervakning som utförs av Polismyndigheten eller Säkerhetspolisen. Den verksamheten är föremål för annan särreglering (se kapitel 18).

[1] Regeringens proposition *En ny kameraövervakningslag*, prop. 2012/13:115 s. 45.

Allmänna krav enligt kameraövervakningslagen

Som ett allmänt krav för kameraövervakning av alla typer av platser gäller att övervakningen ska bedrivas lagligt, enligt god sed och med hänsyn till enskildas personliga integritet. För att kameraövervakning ska vara tillåten krävs vidare, enligt den s.k. överviktsprincipen, att intresset av sådan övervakning ska väga tyngre än den enskildes intresse av att inte bli övervakad. Vid den bedömningen ska särskilt beaktas om övervakningen behövs för att förebygga, utreda och avslöja brott, förhindra olyckor eller något annat jämförligt ändamål – men också hur övervakningen ska utföras, om det används teknik som främjar skyddet av den enskildes personliga integritet samt vilket område som ska övervakas.

Ljud- och bildmaterial som samlats in från kameraövervakning får inte behandlas för något ändamål som är oförenligt med det som materialet samlades in för. Tillgång till materialet får inte ges till fler personer än vad som behövs för att övervakningen ska kunna bedrivas.

Kameraövervakning mot plats dit allmänheten har tillträde

Enligt kameraövervakningslagen krävs som huvudregel tillstånd för att en övervakningskamera ska få vara uppsatt så att den kan riktas mot en plats dit allmänheten har tillträde. Sådana tillstånd ges av länsstyrelserna.

Ett tillstånd till kameraövervakning ska förenas med villkor om hur kameraövervakningen får anordnas. Villkoren ska avse ändamålet med övervakningen, vilken utrustning som får användas och vilket område som får övervakas. Länsstyrelsen ska också besluta om övriga villkor som behövs för tillståndet. Det kan t.ex. handla om vad som ska gälla för upplysning om övervakningen (skyltning) samt hur upptagning, användning, bevarande eller annan behandling av bilder och upptagning av ljud får göras, eller annat som är av betydelse för integritetsskyddet vid övervakningen. Ett tillstånd får meddelas för en begränsad tid.

Innan länsstyrelsen beslutar om tillstånd till kameraövervakning ska i regel kommunen, där övervakningen ska bedrivas, få tillfälle att yttra sig. Kommunen får också överklaga ett beslut om kameraövervakning. Även Datainspektionen får överklaga beslut om kameraövervakning av en plats dit allmänheten har tillträde för att ta tillvara

allmänna intressen. Om kameraövervakningen ska avse en arbetsplats har även en organisation som företräder de anställda på arbetsplatsen rätt att överklaga beslutet.

Från kravet på tillstånd för kameraövervakning gäller ett antal undantag. Undantagen rör bl.a. viss kameraövervakning i trafiken, Polismyndighetens automatiska hastighetsövervakning samt övervakning av vissa i lagen uppräknade skyddsobjekt och av kasinon.

I vissa fall är det tillräckligt med en anmälan för att kameraövervakningen ska vara tillåten. Det gäller i bl.a. bank-, post- och butikslokaler, samt i tunnelbana och parkeringshus. Kameraövervakningen är då endast tillåten för vissa angivna syften – t.ex. för att förebygga, avslöja eller utreda brott, eller förhindra olyckor – och under förutsättning att kameran är fast monterad och försedd med fast optik. Som utgångspunkt gäller också att avlyssning eller upptagning av ljud inte är tillåten utan tillstånd.

Kameraövervakning mot plats dit allmänheten inte har tillträde

När det gäller platser dit allmänheten inte har tillträde krävs varken tillstånd eller anmälan för kameraövervakning. Däremot uppställer kameraövervakningslagen vissa andra krav för att övervakningen ska vara laglig. Kameraövervakning får till att börja med bedrivas om den som ska övervakas har samtyckt till övervakningen. Samtycket ska vara informerat och den övervakade har rätt att när som helst återkalla sitt samtycke. Under vissa förutsättningar är kameraövervakning tillåten även utan samtycke. Det gäller om övervakningen behövs för vissa berättigade ändamål – bl.a. för att förebygga, avslöja eller utreda brott eller förhindra olyckor – och övervakningsintresset väger tyngre än den enskildes intresse av att inte bli övervakad.

Oavsett om kameraövervakningen bedrivs med stöd av samtycke eller överviktsprincipen, krävs därutöver att övervakningen endast få förekomma för särskilda och berättigade ändamål, att ändamålen med övervakningen dokumenteras samt att övervakningen inte används i större omfattning än vad som behövs för att tillgodose ändamålen med övervakningen.

Kameraövervakningslagens övriga regler

Den som bedriver kameraövervakning är i regel skyldig att genom tydlig skyltning eller på något annat verksamt sätt lämna upplysning om övervakningen. Det ska vanligtvis också lämnas en upplysning om vem som bedriver övervakningen. Om ljud kan avlyssnas eller tas upp ska en särskild upplysning lämnas om det.

Vidare finns i kameraövervakningslagen särskilda regler om bl.a. säkerhet för ljud- och bildmaterial, förbud mot överföring av visst material till tredjeland, tystnadsplikt och utlämnande av uppgifter samt skadestånds- och straffansvar i vissa fall. Slutligen finns bestämmelser som reglerar hur länge ljud- och bildmaterial från kameraövervakning får bevaras.

Översyn av kameraövervakningslagen

Regeringen beslutade i november 2015[2] att tillsätta en utredning för att utreda vissa frågor om kameraövervakning. Syftet är att säkerställa att kameraövervakning kan användas där det behövs för att bekämpa brott och samtidigt garantera ett starkt skydd för den personliga integriteten.

Utredaren ska bland annat:

- kartlägga och utvärdera vad kameraövervakningslagen har inneburit för möjligheterna till kameraövervakning och skyddet för den personliga integriteten,
- analysera om möjligheterna till kameraövervakning på särskilt brottsutsatta platser och andra platser med förhöjt skyddsbehov, till exempel asylboenden, medieredaktioner och lokaler som används av religiösa samfund, behöver förbättras,
- undersöka hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom till exempel kamerautrustade drönare, och bland annat ta ställning till om det behövs integritetsstärkande eller teknikfrämjande åtgärder,

[2] Dir. 2015:125.

- ta ställning till om integritetsskyddet på vissa platser dit allmänheten inte har tillträde, till exempel arbetsplatser och skolor, behöver förbättras,
- analysera om integritetsskyddet kan förstärkas genom att Datainspektionen ges föreskriftsrätt när det gäller tillämpningen av kameraövervakningslagen, och
- lämna de författningsförslag som bedöms lämpliga.

Uppdraget ska redovisas senast den 28 februari 2017.

20.1.3 Tillsyn

Länsstyrelserna har ansvaret för tillsynen över kameraövervakning av platser dit allmänheten har tillträde. Tillsynen över kameraövervakning av platser dit allmänheten inte har tillträde utövas däremot av Datainspektionen, som också har ett centralt tillsynsansvar för all kameraövervakning. I den funktionen ingår att utvärdera rättstillämpningen, utvärdera, följa upp och samordna den operativa tillsynen, ge råd och stöd till länsstyrelserna, samt ge information och råd till allmänheten och till de som tillhandahåller och använder övervakningsutrustning. Datainspektionen har också rätt att överklaga länsstyrelsernas beslut i frågor om kameraövervakning, för att tillvarata allmänna intressen.

Länsstyrelserna och Datainspektionen får inom sina respektive tillsynsområden besluta om de förelägganden som är nödvändiga för att kameraövervakningslagen ska följas. Föreläggandena får förenas med vite.

20.2 Användningen av övervakningskameror och därmed jämförbar utrustning

20.2.1 Företeelsen

Olika typer av kameror används för att genom övervakning exempelvis förebygga, avslöja eller utreda brott, eller för att förhindra olyckor. Användningen av sådana kameror innebär dock att enskilda övervakas och därmed också ett intrång i den personliga integriteten.

Traditionella fasta kameror

Traditionell kameraövervakning görs genom att en fast kamera sätts upp på exempelvis en vägg eller en stolpe och därefter används för övervakning av det område som kamerans upptagningsområde täcker. Det kan exempelvis handla om övervakning av en ingång till en lokal, ett rum i en lokal, en tunnelbaneperrong, en parkeringsplats, ett torg eller delar av ett bostadsområde. Bildsignaler och ibland även ljudsignaler skickas från dessa kameror till exempelvis ett kontrollrum eller en dator, där den spelas in och/eller övervakas i realtid. Det förekommer även att bilder från kameror sänds i realtid på internet. Överföringen kan göras analogt i tråd inom ett slutet system, men det är allt vanligare att överföringen görs trådlöst och digitalt via exempelvis internet.

Teknikutvecklingen har även inneburit att kamerorna har blivit mindre och billigare och därför kan användas på fler ställen och i större antal. Samtidigt har kamerornas upplösning ökat, vilket i sin tur har fört med sig att en kamera kan täcka ett område som tidigare krävde många kameror. Den högre upplösningen innebär också att det går att zooma in i bilden utan att bildkvaliteten blir dålig.

Vindrutekameror, drönare och kroppsburna kameror

Utvecklingen av mindre och billigare kameror med hög upplösning har bl.a. medfört att det har blivit allt vanligare att kameror placeras på olika typer av fordon eller farkoster. Det har även utvecklats nya typer av kroppsburna kameror.

Ett exempel på denna utveckling är användningen av s.k. vindrutekameror. En vindrutekamera (på engelska dashboard camera, eller dashcam) är en kamera som sätts fast på ett fordon, exempelvis på insidan av framrutan på en bil, och som spelar in det som händer framför fordonet när det är i rörelse. En sådan inspelning kan bl.a. fungera som bevis vid en olycka, men innebär också att andra fordon och personer som befinner sig framför kameran blir inspelade. Det är dessutom förhållandevis vanligt att sådana inspelningar sprids vidare, t.ex. via internet.

Även drönare har blivit allt vanligare. En drönare är en fjärrstyrd obemannad flygfarkost (t.ex. en helikopter eller ett flygplan) som har varierande räckvidd beroende på tillämpningsområde. Drönare

är numera förhållandevis billiga och används av såväl privatpersoner som myndigheter och företag, bl.a. för att filma och fotografera från luften. Utvecklingen har lett till att drönarna blivit allt mindre. Det ska till och med ha tagits fram drönare i insektsstorlek.[3] Vissa drönare kan filma och fotografera på flera hundra meters avstånd med mycket gott resultat. Det innebär bl.a. att det numera finns ökade möjligheter att filma och fotografera på platser som tidigare varit mycket svårtillgängliga, och utan att den som filmas eller fotograferas upptäcker detta.

En annan trend, inte minst på konsumentmarknaden, är användningen av kroppsburna kameror. Ett av de mest omskrivna exemplen i denna kategori är Googles dator- och kameraförsedda glasögon Google Glass, som bl.a. kan filma och fotografera i smyg. Det finns även små kameror som är avsedda att fästas på kläderna och som filmar eller kontinuerligt, exempelvis var trettionde sekund, tar bilder av bärarens omgivning utan att de som filmas eller fotograferas märker detta.

20.2.2 Risker för den personliga integriteten

Kameraövervakning förekommer på många platser och kan bl.a. bidra till att förebygga, avslöja och utreda brott. Den kan också bidra till att skapa trygghet (faktisk eller upplevd) för enskilda. Det kan i sin tur leda till att fler människor vistas på platsen och att den sociala kontrollen ökar, vilket kan minska risken för brott. Kameraövervakning kan också vara användbart för andra ändamål, t.ex. för att förhindra olyckor, kontrollera hur personer förflyttar sig inom ett övervakat område eller för att kartlägga vilka kunder som besöker t.ex. ett varuhus, eller vilka varor kunder tittar på i en butik, genom att t.ex. följa deras ögonrörelser.

Det är i viss utsträckning osäkert hur stor den faktiska effekten av kameraövervakning verkligen är. Det finns studier som tyder på att kameraövervakning förebygger många brott på exempelvis parkeringsplatser, men att effekterna är både svagare och mindre säkra på andra typer av platser.[4] I Brottsförebyggande rådets (Brås) senaste

[3] *Is that really just a fly? Swarms of cyborg insect drones are the future of military surveillance*, artikel den 19 juni 2012 i MailOnline.

[4] Se bl.a. Brottsförebyggande rådets rapport *Kameraövervakning och brottsprevention – En systematisk forskningsgenomgång (2007:29)*.

delrapport angående ett pågående försök med kameraövervakning vid Stureplan och Medborgarplatsen i Stockholm, konstateras t.ex. att utvärderingen inte ger något stöd för att kameraövervakningen har haft någon effekt på vare sig brottsligheten eller tryggheten på de två platserna.[5] Samtidigt noterar Brå att många av besökarna på just dessa platser inte ens känner till att det pågår kameraövervakning där, vilket påverkar resultatet av undersökningen. Brå framhåller dessutom att inspelningar från kameraövervakning kan bidra vid utredning av brott.

Samtidigt innebär kameraövervakning ett påtagligt intrång i den enskildes integritet. I och med att övervakningen avser en viss plats och inte en viss individ, ligger det dessutom i sakens natur att den även omfattar personer och handlingar som det egentligen inte finns skäl att övervaka. Ett exempel på detta är att man vid kameraövervakning som syftar till att förebygga skadegörelse, inbrott och stölder på en skola även kan följa allt annat som eleverna gör på skolan samt vad lärarna gör och till och med hur av skolan anlitade entreprenörer (exempelvis en anlitad städfirma) fullföljer sina uppdrag.[6] Kameraövervakning innebär alltså att ett mycket stort antal personer övervakas i sina dagliga aktiviteter.

Genom sammankoppling av kamerasystem är det numera möjligt att övervaka mycket stora områden och följa nästan allt som enskilda gör inom dessa områden. Riskerna för den personliga integriteten ökar successivt i takt med utbyggnaden av sammankopplade kamerasystem.

Det finns också en risk för att övervakningen bedrivs utan att de som övervakas känner till det och kan välja att vistas någon annanstans. Om övervakningen dessutom pågår utan föregående ansökan eller anmälan, minskar även tillsynsmyndighetens möjligheter att upptäcka eventuella överträdelser.

Under år 2013 genomförde 19 av landets 21 länsstyrelser en gemensam tillsyn av kameraövervakningen hos sammanlagt 116 gallerior och 693 butiker, dvs. totalt 809 objekt, för att undersöka hur gällande regler och villkor efterföljs. Av rapporten från granskningen framgår att 327 av dessa objekt, dvs. cirka 40 procent, fick

[5] Brottsförebyggande rådets rapport *Kameraövervakning på Stureplan och Medborgarplatsen, Delrapport 2* (2014:12).

[6] Jfr Datainspektionens dnr 476-2009, som gällde just användning av inspelningar från en sådan kamera för att bedöma hur en extern städfirma fullgjorde sitt uppdrag.

någon typ av anmärkning.[7] En förhållandevis stor del av anmärkningarna avsåg otillåten kameraövervakning i eller utanför butiker, t.ex. att anmälan eller tillstånd saknades eller att kameran var felriktad. En annan vanlig brist var att butikerna inte följde reglerna om skyltning.

Under 2014 genomförde 20 länsstyrelser en liknande gemensam tillsyn av den kameraövervakning som bedrevs på sammanlagt 195 vårdinrättningar, bl.a. sjukhus och vårdcentraler. Av rapporten från den granskningen framgår att 57 av dessa objekt, dvs. cirka 27 procent, fick någon typ av anmärkning.[8] De vanligaste anmärkningarna var även vid denna granskning att tillstånd för övervakningen saknades eller att vårdinrättningarna inte följde reglerna om skyltning.

Vid övervakning med hjälp av vindrutekameror, drönare och kroppsburna kameror är risken naturligtvis ännu större att de övervakade inte känner till det (jfr t.ex. kameraövervakningslagens krav på skyltning).[9] Med drönare är det dessutom möjligt att övervaka svåråtkomliga platser, exempelvis trädgårdar och andra utrymmen där man inte har anledning att tro att man är övervakad. Även om man som enskild vet att det finns drönare i området kan det vara svårt att veta vem som samlar in vilken information och vad syftet med insamlingen är, vilket kan leda till en känsla av att ständigt vara övervakad och att man avstår från att utöva vissa rättigheter (s.k. chilling effect). Användningen av kroppsburna kameror kan dessutom medföra att man oavsiktligt råkar fotografera eller filma sådant som man varken bör eller får spela in. Den som bär en kroppsburen kamera kan t.ex. glömma att stänga av den när han eller hon går in i ett omklädningsrum eller på en plats där det råder fotoförbud.

När det gäller vindrutekameror och drönare har det diskuterats om kamerorna kan anses vara varaktigt uppsatta och därmed omfattas av kameraövervakningslagen, eller om det i stället är personuppgiftslagen som är tillämplig på sådan övervakning. Frågan är för närvarande föremål för prövning i olika domstolar vilket förhoppningsvis kommer att

[7] Se länsstyrelsernas rapport *Tillsyn av kameraövervakning över gallerior/köpcentrum och dess verksamheter 2013*.

[8] Se länsstyrelsernas rapport *Länsstyrelsernas tillsyn av kameraövervakning 2014.*

[9] Se t.ex. Artikel 29-gruppens ”Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones”, av den 16 juni 2015.

leda till att rättsläget blir tydligare.[10] Hösten 2015 kom två kammarrättsavgöranden där de drönare som bedömdes ansågs vara uppsatta i kameraövervakningslagens mening.[11]När det gäller kroppsburna kameror har Datainspektionen dock gjort bedömningen att de faller utanför kameraövervakningslagens tillämpningsområde.

I och med att signalerna allt oftare överförs trådlöst, exempelvis via internet, finns en risk att obehöriga bereder sig tillgång till signalerna. Detta är ett problem när det gäller många enklare produkter, s.k. nätverkskameror, som marknadsförs mot privatpersoner och mindre företag. Ett bristfälligt säkerhetsmedvetande hos användaren kan också bidra till problemet. Se även nedan angående lagring och automatisk bildanalys.

20.3 Lagring och automatisk bildanalys

20.3.1 Företeelsen

Övervakningskameror kan, som framgått ovan, inte bara användas för att övervaka ett händelseförlopp i realtid, utan bild och ljud kan också spelas in. Det inspelade materialet kan därefter lagras och analyseras. Analysen kan vara helt eller delvis automatisk, och bl.a. innebära att de inspelade uppgifterna samkörs med annan information.

Lagring

Inspelningar av bild och ljud görs numera digitalt, vilket bl.a. medför att stora mängder inspelat material kan lagras förhållandevis billigt på hårddiskar eller andra lagringsformat. Det finns därför inte samma ekonomiska incitament som tidigare att begränsa mängden inspelat material genom exempelvis gallring. Det har också blivit allt vanligare att lagra bild och ljud hos någon annan, exempelvis i det s.k. molnet (se vidare kapitel 21). Den som gjort inspelningen har därför

[10] Se bl.a. Kammarrättens i Stockholm mål nr 5394-15 (överklagande av Förvaltningsrätten i Stockholms dom den 20 maj 2015 i mål nr 10208-15), Kammarrättens i Jönköping mål nr 1369-15 (överklagande av Förvaltningsrättens i Linköping dom den 23 april 2015 i mål nr 2020-15) samt Högsta förvaltningsdomstolens mål nr 4110-15 (överklagande av Kammarrättens i Göteborg dom den 10 juni 2015 i mål nr 1674-15).

[11] Kammarrättens i Göteborgs dom den 2 november 2015, mål nr 2156-15 och Kammarrättens i Jönköping dom den 15 december 2015, mål nr 1369-15

inte samma kontroll som tidigare över vem som kan få del av materialet. Även rent interna nätverk är allt oftare konstruerade så att lagrad information är åtkomlig via exempelvis internet, ibland med hjälp av lösenord.

Automatisk bildanalys

En dator som är inbyggd i kameran, eller som senare får tillgång till digitala stillbilder eller filmer, kan i viss utsträckning räkna ut vad som syns på bilden eller filmen. Datorn kan avgöra om det finns ett mänskligt ansikte på bilden eller inte. En vanlig metod för sådan analys är att datorn instrueras att leta efter mörka och ljusa rektanglar i vissa kombinationer. Dessa rektanglar fungerar som kraftiga förenklingar av hur ögon, näsa, mun och andra delar i ett ansikte ser ut. En lång, mörk horisontell rektangel med en ljus direkt under kan vara ögonen och kinderna, en ljus rektangel mellan två mörka kan vara näsan. När flera sådana matchningar finns i bilden, med rätt placering i förhållande till varandra, är sannolikheten stor att det är ett mänskligt ansikte.

Samma grundprincip gäller för all automatisk bildigenkänning; datorn letar efter kända mönster i bilden. Möjligheten att automatiskt klassificera vad som händer framför kameran skapar nya förutsättningar för kameraövervakning. Den gör det t.ex. möjligt att automatiskt upptäcka att en människa befinner sig i en del av kamerans synfält där människor inte får vistas, eller att en väska har stått lämnad väldigt länge. Den gör det även möjligt för datorn att automatiskt läsa av text, exempelvis registreringsnumret på ett fordon, som passerar framför kameran.

Det går till och med att skapa regler för att datorn ska känna igen specifika personer. Datorn får då öva på ett antal bilder av personen som den ska känna igen, och med utgångspunkt från dessa skapa regler som beskriver just den personens karaktäristiska utseende. Vid denna typ av analys är området kring ögonen, bl.a. ögonbryn, ögonlock och hur djupt ögonen sitter, av särskild betydelse. Metoden används i vissa bildbehandlingsprogram (t.ex. Photoshop) och i vissa

länder även av Facebook.[12] Den används även av myndigheterna i vissa länder, bl.a. för att identifiera misstänkta brottslingar. Identifiering av specifika personer kan också göras via s.k. gait analysis, dvs. genom en jämförelse med en persons unika rörelsemönster, eller med hjälp av kameror som förmår att på håll fotografera och analysera människors irisar, utan att personen som ska identifieras är medveten om det.

Vad en dator tränas att känna igen beror på syftet med installationen och hur informationen som skapas ur analysen ska användas. I vissa fall kan identifieringen av den som rör sig framför kameran underlättas genom att övervakningssystemet kopplas till andra databaser. Vid ansiktsigenkänning förekommer det t.ex. att personer i det övervakade området automatiskt jämförs med fotografier av kända individer i en databas. Även annan information kan användas för att underlätta identifieringen. Om det övervakade området exempelvis är utrustat med ett inpasseringssystem där personer använder en personlig kod eller ett passerkort för att ta sig in, kan den informationen användas för att identifiera eller underlätta identifiering av de personer som syns på bilden.

En dator kan dessutom instrueras att agera på visst sätt när den observerar något som den är programmerad för. Sådana kameror kallas ibland intelligenta kameror. Det kan handla om att datorn ska larma ett vaktbolag när en människa befinner sig på förbjudet område, eller att datorn ska avidentifiera personer på bild genom att t.ex. lägga till en kvadrat över deras ansikten eller ersätta dem med streckgubbar. Det sistnämnda är ett exempel på hur teknikutvecklingen också har medfört ökade möjligheter att begränsa riskerna för integritetsintrång. Det finns även andra typer av händelsestyrda kameror, exempelvis kameror som börjar sända bilder till ett vaktbolag när ett rök- eller rörelselarm har aktiverats, så att personalen kan se vad det är som utlöst larmet. Den typen av kamerasystem kan även kopplas samman med exempelvis ett system som automatiskt

[12] Facebook har tagit bort denna funktion för användare inom EU, efter en rekommendation från Irlands dataskyddsombudsman (Data Protection Commissioner, DPC). Se bl.a. http://www.dataprotection.ie/docs/21/09/12_Press_Release_-Facebook_Ireland_Audit_Review_Repor/1233.htm. Facebook arbetar för närvarande också med att ta fram ett nytt ansiktsigenkänningssystem, DeepFace, som enligt uppgift ska kunna känna igen ansikten med mycket stor precision (Why Facebook is beating the FBI at facial recognition, artikel publicerad den 7 juli 2014 i The Verge).

stänger dörrar vid brandlarm. Dessa kameror gör det alltså enklare att snabbt vidta rätt åtgärd, vilket minskar risken för person- och sakskador.

Tekniken kan också användas för statistiska eller kommersiella ändamål, t.ex. för att se hur enskilda personer rör sig i en butik, genom att följa hur de, som befinner sig framför kameran eller kamerorna, förflyttar sig i det övervakade området. Det är även möjligt att följa kundernas ögonrörelser och därmed registrera vilka varor en kund tittar på i en butiks hyllor.

Den automatiska analysen görs i regel med viss fördröjning, genom analys av inspelat eller lagrat material. Det finns dock även teknik för automatisk analys i realtid, och det pågår arbete för att ytterligare utveckla sådan teknik. Ett uppmärksammat exempel är Google Glass-appen NameTag, som kan skanna av personer som användaren möter och i realtid hämta information om dem från en databas.[13]

Ett annat exempel är det kamerasystem för automatisk avläsning av registreringsskyltar (Automatic Number Plate Recognition, nedan ANPR) som har installerats i ett antal polisbilar runt om i Sverige. Detta system läser av skyltar på fordon i närheten och jämför dessa mot vägtrafikregistret och registret för efterlysta fordon. Om datorn upptäcker att en bil i närheten är exempelvis stulen, obesiktigad eller har körförbud, informeras polispatrullen automatiskt och kan stoppa det aktuella fordonet för en närmare kontroll.

Ett antal säkerhetsbolag har ansökt om att få använda en liknande teknisk lösning för att förhindra obetalda tankningar. Systemet innebär att en kamera vid bensinstationens infart automatiskt läser av registreringsnummer för fordon som kör in på bensinstationen. Därefter jämförs dessa registreringsnummer automatiskt med registreringsnummer för fordon som tidigare tankats utan betalning och som därför har registrerats i en databas. Om fordonet finns

[13] Tekniken skulle bl.a. kunna användas av brottsbekämpande myndigheter. Som exempel kan nämnas att polismyndigheten i Dubai tidigare haft planer på att förse patrullerande poliser med Google Glass för att möjliggöra automatisk ansiktsigenkänning (*Dubai detectives to get Google Glass to fight crime*, artikel publicerad den 2 oktober 2014 av Reuters). Google har för tillfället har stoppat försäljningen av Google Glass, men uppgett att produkten kommer att finnas kvar och fortsätta utvecklas (*Google Glass sales halted but firm says kit is not dead*, artikel publicerad den 15 januari 2015 av BBC).

registrerat i databasen får personal på bensinstationen uppgift om detta och kan besluta om fordonsföraren ska tillåtas tanka på kredit eller om tankningen måste förskottsbetalas.[14]

Det förekommer även att företag i kommersiella syften, exempelvis vid köpcenter, använder kameror för att läsa av registreringsskyltar på kundernas bilar för att kunna identifiera individer och visa riktad reklam i direkt anslutning till bilen.[15] Vidare finns exempel på hur bilder av registreringsskyltar samlas in och lagras i databaser för att bl.a. säljas vidare till olika företag och myndigheter.[16]

20.3.2 Risker för den personliga integriteten

Vid lagring av integritetskänslig information finns det alltid en risk för obehörig åtkomst till – och olovlig spridning av – informationen.

Tryckfrihetsförordningens och yttrandefrihetsgrundlagens bestämmelser om meddelarfrihet har företräde framför kameraövervakningslagens regler om tystnadsplikt. Om bilder från kameraövervakning olovligen lämnas ut för ett offentliggörande enligt någon av dessa lagar, får det allmänna i regel inte ingripa mot utlämnaren av bilderna.[17] I den situationen är det i regel inte heller möjligt att hålla den ansvariga utgivaren ansvarig för efterföljande offentliggörande på t.ex. en dagstidnings webbplats.

Vidare kan bristande säkerhet avseende material från kameraövervakning, exempelvis när det gäller interna rutiner för åtkomstkontroll, loggning, kryptering, anonymisering och gallring, få stora konsekvenser för enskilda. Om uppgifterna lagras hos någon annan, t.ex. på någon typ av molntjänst, kan även bristande säkerhet hos denna samarbetspartner få stora konsekvenser.

[14] Högsta förvaltningsdomstolen biföll Datainspektionens överklagan i dom den 16 februari 2016 ansökan (mål nr 4970-14). Domstolen fann att syftet med behandlingen inte kan anses motivera det integritetsintrång som behandlingen innebär. Det saknades således skäl att i det aktuella fallet medge undantag från förbudet att behandla personuppgifter om lagöverträdelser som innefattar brott.

[15] Datainspektionens beslut den 1 maj 2012, dnr 1874-2011.

[16] Se vidare *Massive license plate location database just like Instagram, Digital Recognition Network insists*, artikel den 5 mars 2014 i The Boston Globe.

[17] Justitiekanslerns beslut den 22 november 2002, dnr 2907-02-30.

Som tidigare nämnts i avsnitt 20.2.2 genomförde 20 länsstyrelser under år 2014 en gemensam tillsyn av den kameraövervakning som bedrevs på sammanlagt 195 sjukhus, vårdcentraler och andra vårdinrättningar. Av rapporten från den granskningen framgår bl.a. att inspelat material i vissa fall lagrades alltför länge.

När stora datamängder är lagrade finns vidare en risk att uppgifterna till slut används på ett sätt som är oförenligt med det syfte för vilket uppgifterna samlades in.

Om bilder eller filmer samkörs med annan information om den enskilde, blir intrånget i den enskildes integritet genast större. Sådan samkörning kan möjliggöra omfattande kartläggning av enskilda. Någon som använder kameror med möjlighet till ansiktsigenkänning för att identifiera personer på gatan skulle, genom samkörning med olika databaser i realtid kunna få information om personens yrke, bostadsadress, ekonomiska och familjeförhållanden samt bekantskapskrets och hobbyer m.m.

Vid sådan samkörning finns dessutom risken att den externa datakällan har bristande kvalitet eller innehåller inaktuell information. Om den externa datakällan finns på annan plats, är även kommunikationen med datakällan ofta exponerad för samma risker som andra överföringar via internet. Det gäller t.ex. risken att någon obehörig tar del av informationen. Denna risk är särskilt stor om tydliga riktlinjer för åtkomst och gallring saknas.

När tekniken används för att skydda den personliga integriteten, exempelvis vid automatisk anonymisering av resultatet från kameraövervakning, bör man vara medveten om att det finns en risk att de algoritmer (regler) som används inte är felfria och att visst material därför inte blir avidentifierat.

20.4 Kommitténs samlade bedömning av området

Diskussionen om kameraövervakning och personlig integritet är på intet sätt ny. De senaste årens teknikutveckling har dock ändrat förutsättningarna för övervakningen och aktualiserat nya aspekter. Det finns anledning att anta att teknikutvecklingen även har inneburit att kameraövervakningen i samhället har ökat väsentligt. I dagsläget är det dock ingen myndighet som har en samlad bild över hur omfattande kameraövervakningen är. Det finns inte ens någon samlad

statistik avseende sådan kameraövervakning som kräver tillstånd eller anmälan. Denna avsaknad av statistik är en brist som gör det svårt att upptäcka förändringar när det gäller användningen av kameraövervakning. Avsaknaden gör det också svårt att bedöma hur omfattande kameraövervakningen faktiskt är.

Redan den omständigheten att kameraövervakning förekommer anses innebära ett intrång i den personliga integriteten, även om övervakningen endast görs i realtid och ingen inspelning förekommer. Om övervakningen spelas in blir intrånget större, beroende på hur länge materialet bevaras, vilka som har tillgång till det och vad det används till. Om olika kamerasystem kopplas samman med varandra eller om inspelade bilder kopplas samman med information i stora databaser och biometriska funktioner som t.ex. ansiktsigenkänning, möjliggörs en omfattande kartläggning och intrånget i den personliga integriteten kan bli mycket stort. Det ökade antalet kameror, även bland privatpersoner, i kombination med bättre upplösning, billigare lagringsutrymme och möjligheterna till samkörning med uppgifter i andra databaser, innebär stora risker för intrång i den personliga integriteten. Med drönare och kroppsburna kameror är det dessutom större risk än tidigare att man, avsiktligt eller oavsiktligt, filmar känsliga situationer, exempelvis i en trädgård eller ett omklädningsrum. Därtill kommer risken för publicering eller annan otillbörlig spridning av bilder, som ofta innebär ett särskilt stort intrång i den personliga integriteten. När det gäller etablerade former för kameraövervakning finns dock ett skyddande regelverk och en aktiv tillsyn. För närvarande pågår en översyn av kameraövervakningslagen och hur den ska förhålla sig till den nya tekniken. Kommittén gör bedömning att kameraövervakning innebär påtagliga risker för den personliga integriteten.

Kameraövervakningen har övergått från fysiskt avgränsade analoga system till uppkopplade datoriserade installationer. Tekniken utsätts därför för samma typer av risker som alla andra it-system. Det innebär bl.a. att det material som kamerorna överför eller spelar in måste skyddas från intrångsförsök från utsidan och att innehållet måste skyddas från avlyssning när det överförs från kameror till servrarna där materialet lagras. Används s.k. molntjänster uppkommer ytterligare säkerhetsproblem.

Vid lagring av omfattande material ökar också risken för s.k. ändamålsglidning, dvs. för att materialet kommer till annan användning än den för vilken inspelningen ursprungligen gjordes.

Lagring, bildanalys och annan vidareanvändning av bilder och film ökar alltså riskerna som är förknippade med kameraövervakning. Kommittén bedömer därför att lagring och vidarebearbetning av sådana uppgifter är förknippade med allvarliga risker för den personliga integriteten.

Kamerövervakningslagen har till syfte att tillgodose behovet av kameraövervakning, men också att samtidigt skydda enskilda mot otillbörliga intrång i den personliga integriteten. För att åstadkomma detta skydd innehåller lagen detaljerade bestämmelser om när kameraövervakning är tillåten samt om upplysningsplikt, säkerhet och bevarande av material. Som framgår ovan är det ännu inte helt klarlagt om den regleringen är tillämplig vid användning av vindrutekameror och drönare, vilket i sig är en risk för den personliga integriteten. Det kan även i andra fall vara svårt för en enskild att avgöra om en planerad övervakning omfattas av kameraövervakningslagen, eller om verksamheten anses vara av rent privat natur.[18]

Sammantaget är kameraövervakning ett område där det finns särskild anledning att följa den tekniska utvecklingen, t.ex. i fråga om möjligheter att koppla samman kamerasystem och databaser samt när det gäller risker för otillåten spridning och annat missbruk av material.

[18] Jfr EU-domstolens dom den 11 december 2014 i mål nr C-212/13.

21 Några särskilda företeelser

21.1 Molntjänster

Kommitténs bedömning: Publika molntjänster där flera leverantörer är inblandade, innebär allvarliga risker för den personliga integriteten.

21.1.1 Företeelsen

Begreppen molnet och molntjänster används som gemensamt namn för tjänster som ersätter program och lagringsutrymme i användarens egen dator och i stället erbjuder motsvarande funktioner via internet. Beteckningen molnet har hämtats från illustrationer över datorkommunikation, där just ett moln ofta används som symbol för internet.

I begreppet molntjänster ryms en stor bredd av tjänster. De risker som utmärker molntjänsterna är större om det rör sig om tjänster som innebär att uppgifter hanteras av multinationella företag med verksamhet utanför EES. I det här kapitlet ligger därför fokus på globala molntjänster, snarare än på nationella molntjänster. Fokus ligger vidare på tjänster som riktar sig mot företag, myndigheter och organisationer, och inte i första hand till privatpersoner. Molntjänster som riktar sig till privatpersoner avhandlas på andra ställen, såsom i kapitlen om sociala medier och e-post (kapitel 13) respektive om hälso- och sjukvård och socialtjänst (kapitel 9).

I september 2011 publicerade NIST (National Institute of Standards and Technology) i USA en än i dag ofta citerad, generell beskrivning av vad molntjänster är. I texten räknar NIST upp fem karaktärsdrag hos molntjänster: [1]

1. självbetjäning är möjlig när kunden behöver det,
2. åtkomst sker via nätet i olika klienter (exempelvis stationära datorer, mobiltelefoner och surfplattor),
3. kunden delar leverantörens resurser med andra kunder,
4. prestanda anpassas till kundens behov för stunden, och
5. tjänsterna går att mäta, bl.a. i syfte att avgöra hur mycket kunden ska debiteras för tjänsten.

Man brukar tala om fyra olika typer av molntjänster: publika moln, partnermoln, hybridmoln och privata moln.[2]

Publika molntjänster ägs och hanteras av en molntjänstleverantör (tredje part) som säljer resurser till flera kunder i samma infrastruktur. Tjänster i publika moln är potentiellt tillgängliga för alla som så önskar. Exempel på publika molntjänster är GoogleApps, iCloud och Dropbox.

Partnermoln, som ibland också kallas för gemenskapsmoln eller branschmoln, erbjuds till en begränsad och väldefinierad grupp av kunder. En särskild form av partnermoln är s.k. myndighetsmoln. Ett myndighetsmoln har skapats i t.ex. Storbritannien, för att möta särskilda behov av t.ex. säkerhet.

Privata molntjänster bygger på en infrastruktur som är dedikerad åt endast en användare. Infrastrukturen kan hanteras av användaren själv eller av en annan aktör.

Termen *hybridmoln* avser en sammansättning av två eller flera molntyper som möjliggör kopplingar mellan olika tjänster och molntyper. Ett exempel på hybridmoln är Tieto Productivity Cloud.[3]

---

[1] *The NIST Definition of Cloud Computing*, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800–145.

[2] Den följande beskrivningen av molntyperna är i allt väsentligt hämtad från Pensionsmyndighetens rapport *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015.

[3] Produktinformation med titeln *Därför är hybridmoln bästa lösningen*, läst på www.tieto.se den 8 april 2016.

En konsekvens av tekniken bakom molntjänsterna är att organisationens information läggs i händerna på tjänsteleverantören. Värt att uppmärksammas är att det sällan är klart hur och var informationen lagras. Hos de globala molntjänstleverantörerna lagras uppgifterna dock oftast i ett s.k. tredje land, d.v.s. i länder utanför EES-området, som vanligen har en lagstiftning som ger sämre skydd än EU:s dataskyddsdirektiv. De stora molntjänstleverantörerna använder sig vanligtvis också av underleverantörer, vilka i sin tur kan ha underleverantörer som är spridda över hela världen. Den som hanterar sin information i molnet förlorar därför som regel den absoluta kontrollen över informationen. Molntjänster kännetecknas av att informationen flödar över nationsgränserna på ett sätt som är omöjligt för en molnkund att överblicka och än mindre kontrollera. Informationen kan finnas på ett datacenter i Europa på förmiddagen och på andra sidan jordklotet vid midnatt.[4]

Fördelar med molntjänster

Molntjänster erbjuder många fördelar för kunderna. Det handlar bland annat om en tydlig kostnad. Organisationen behöver inte investera i egen hård- och mjukvara utan kan i stället betala per användare. Kapacitet efter behov är också en fördel. Kunden behöver då inte köpa utrustning som går att växa i, utan bara betala för det dagsaktuella behovet. För mindre organisationer innebär molntjänster att de kan fokusera på kärnverksamheten. För näringslivet har framväxten av molntjänster inneburit att nystartade företag inte behöver göra stora investeringar i hårdvara.

I sin vägledning *Använd molntjänster på rätt sätt* listar Sveriges Kommuner och Landsting tre fördelar med molntjänster. De beskrivs som kostnadseffektiva, behovsanpassade och lämpade för mobila arbetssätt.

Driftssäkerhet är en ytterligare fördel med molntjänster som lyfts fram av Enisa (European Union Agency for Network and Information Security) i en rapport om incidentrapportering för molntjänster.[5]

[4] *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015.
[5] *Cloud Security Incident Reporting – Framework for reporting about major cloud security incidents*, utgiven av Enisa i december 2013.

I rapporten används Japan som exempel. Efter den stora jordbävningen år 2011 har man allt mer arbetat med molnlösningar, eftersom man ser det som ett sätt att bygga infrastruktur som står emot naturkatastrofer, tack vare möjligheterna att bygga datorhallar på flera olika platser. Enisa konstaterar också att molntjänster som används på rätt sätt har potential att ge bättre skydd mot överbelastningsattacker. Samtidigt kan en koncentration av it-resurser till ett fåtal stora datacenter innebära att cyberattacker mot dessa kan få stora följder för samhället.

Till fördelarna med en flytt till molnet hör också tjänsteleverantörens expertkunskaper, vilka kan medföra att uppgifterna får ett bättre skydd hos molntjänstleverantören än hos den personuppgiftsansvarige kunden, under förutsättning att kunden förmår ställa rätt krav på leverantören.

Framtiden för molntjänster

I december 2014 presenterade Statistiska centralbyrån en rapport om företagens it-användning. Rapporten visar bland annat att fyra av tio svenska företag köper molntjänster och ungefär hälften så många använder gratistjänster. De vanligaste tjänsterna som företag betalar för är fillagring och e-post.[6]

Prognoser för framtiden beskriver närmast unisont en stark tillväxt för molntjänster på alla fronter. Ett exempel på en sådan prognos är en rapport från analysföretaget IDG Enterprise Research, som genomfört en enkätundersökning med 1 672 it-beslutsfattare runt om i världen. De tillfrågade beslutsfattarna räknade med att hantera 53 procent av sina it-miljöer i molnet i slutet av år 2015. Vidare räknade man med att lägga en fjärdedel av sina budgetar på molntjänster av olika slag.[7]

Samtidigt finns det siffror som tyder på att Edward Snowdens avslöjanden om USA:s massövervakning kommer att få och redan har haft negativa effekter på kundernas benägenhet att anlita molntjänstleverantörer som är baserade i USA. Storleken på effekten

[6] *Företagens användning av it 2014*, Statistiska centralbyrån 2014.
[7] Martin Wallström, Molnflytten ökar takten, publicerad den 28 november 2014 på www.idg.se.

varierar i olika bedömningar, exempelvis uppskattar en bedömare de sammanlagda förlusterna för amerikanska företag till mellan 22 och 35 miljarder dollar över en treårsperiod.[8]

Ett exempel på en i Sverige mycket vanlig molntjänst är Googles Google Apps for Education för skolan. Våren 2014 genomförde SVT Västnytt en enkätundersökning bland landets 290 kommuner, varav 123 svarade att de i någon form använder tjänsten. En annan mycket vanlig molntjänst i svenska skolor och högskolor är Microsofts Office 365 som också används av bl.a. Sveriges television.

Pensionsmyndigheten har på uppdrag av regeringen analyserat och värderat potentialen för användning av molntjänster i staten och redovisat vilka risker och hinder som finns förknippade med användning av molntjänster i statlig verksamhet.[9] Mycket av det som sägs i rapporten gäller för molntjänster i allmänhet, även om rapporten är skriven ur statlig synvinkel. De potentiella säkerhetsrisker som tas upp i rapporten är bristande insyn och kontroll, otydlighet i ansvar och roller, avvikelser mellan krav och leverans, permanent förlust av data, obehörig åtkomst, risker med delad miljö, otillgängliga molntjänster, kompetensförlust, inlåsning, förändringar i leverantörsförhållanden och inkompatibla säkerhetslösningar. De flesta av dessa risker är relevanta för integritetsskyddet. Vi återkommer till detta i avsnittet nedan om kommitténs samlade bedömning av området.

Även fördelarna för statliga verksamheter med användningen av molntjänster beskrivs i rapporten. Molntjänster erbjuder potentiella fördelar som exempelvis kostnadsbesparingar och möjlighet till förbättrade tjänster och verksamhetsresultat i myndigheter. Vidare sägs att en övergång till molntjänster i många fall också kan innebära att säkerheten förbättras på olika sätt, exempelvis genom bättre säkerhetslösningar eller högre kompetens inom säkerhetsområdet hos leverantören än hos kunden.

Avslutningsvis föreslår Pensionsmyndigheten i rapporten åtta åtgärder för regeringen.

1. Uppdra till svenska myndigheter att analysera hur de kan använda molntjänster för att utveckla verksamheten och göra sig beredda att övergå till molntjänstleveranser – beredda att bli ”cloud ready”.

[8] Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?*, augusti 2013, The Information Technology and Innovation Foundation.

[9] *Molntjänster i staten*, *En ny generation av outsourcing*, Pensionsmyndigheten, 2015.

2. Inrätta ett kompetenscenter för anskaffning och användning av externa it-tjänster, dit både verksamhetsföreträdare och upphandlare kan vända sig och där även frågor från privata aktörer kan besvaras.
3. Analysera myndigheters digitala mognad. Undersök i vilken mån de har anlagt ett strategiskt perspektiv på molntjänster för sin egen verksamhet, grad av organisatorisk mognad och operativ beredskap för användning av molntjänster.
4. Fördjupa analysen avseende statliga myndighetsmoln. Undersök intresse och förutsättningar för att inrätta ett eller flera separata myndighetsmolntjänster, s.k. ”gov cloud”. Detta skulle kunna ge möjligheter att förenkla användningen av molntjänster även då det är sekretessbelagd information som hanteras.
5. Utred närmare om det är lämpligt och ändamålsenligt att införa en lagreglerad och straffsanktionerad tystnadsplikt för privata leverantörer.
6. Prioritera att se över myndigheternas registerförfattningar och genomför nödvändiga författningsförändringar för att säkerställa bättre förutsättningar för myndigheterna att utföra sina uppdrag på ett effektivt och rättsäkert sätt.
7. Ge Myndigheten för samhällsskydd och beredskap i uppdrag att genomföra en riskanalys av användning av molntjänster och andra externa it-tjänster ur ett nationellt perspektiv, och att föreslå eventuella åtgärder.
8. Intensifiera Sveriges närvaro i frågor som rör molntjänster i EU och andra internationella sammanhang. Ett tvärpolitiskt arbetssätt som stöder olika politikområden rekommenderas.

21.1.2 Det skyddande regelverket

För att den personuppgiftsansvarige överhuvudtaget ska kunna behandla personuppgifter krävs att det finns ett stöd för behandlingen i personuppgiftslagen (1998:204) eller annan registerförfattning.

Dessutom finns det i personuppgiftslagen vissa krav som är särskilt viktiga om den personuppgiftsansvarige anlitar ett biträde som hanterar uppgifterna i en molntjänst. Till att börja med är bestämmelserna i 30 § personuppgiftslagen om personuppgiftsbiträdesavtal centrala. Andra viktiga bestämmelser för molntjänster är 31 § personuppgiftslagen om säkerhetsåtgärder samt 33–35 §§ personuppgiftslagen om överföring av personuppgifter till tredje land.

För statliga myndigheter gäller även Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

Datainspektionen har i flera tillsynsärenden utvecklat hur bestämmelserna i personuppgiftslagen ska tillämpas på molntjänster.[10]

Ändamål med behandlingen

Av 30 § personuppgiftslagen framgår att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal (personuppgiftsbiträdesavtal) om biträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att biträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de säkerhetsåtgärder som anges i 31 § första stycket personuppgiftslagen.

Enligt Datainspektionen ska instruktionerna enligt 30 § personuppgiftslagen till biträdet om ändamålen med behandlingen utgå ifrån den personuppgiftsansvariges ändamål med sin tänkta hantering av personuppgifter. Instruktionerna får inte omfatta befogenhet för biträdet att exempelvis behandla personuppgifterna på ett sätt som inte skulle vara tillåtet för den ansvarige.

[10] Se exempelvis Datainspektionens beslut den 31 maj 2013 i ärendet 1351-2012, vilket efter överklagande fastställdes av Förvaltningsrätten i Stockholm (mål nr 15410-13). Ärendet rörde en kommuns användning av molntjänsten Google Apps med funktioner för e-post och kalender både för kommunens anställda och för elever i kommunens skolor.

Artikel 29-gruppen pekar i sitt yttrande om molntjänster på att det inte är ovanligt att ett typiskt molnscenario omfattar ett stort antal underentreprenörer. Risken för att personuppgifter kan komma att behandlas för andra, oförenliga ändamål måste därför enligt yttrandet, betraktas som ganska stor.

Radering

Vidare måste instruktionerna enligt 30 § personuppgiftslagen innehålla bestämmelser för biträdet om radering av personuppgifter. Enligt Datainspektionen ska instruktionerna ha som utgångspunkt att när den ansvarige har markerat personuppgifter för radering ska biträdet inom en rimlig tidsperiod påbörja slutlig radering av informationen i fråga. När personuppgifter har markerats för radering får de således inte längre behandlas på annat sätt än som ett led i raderingsprocessen.

Radering av uppgifter innebär här antingen att uppgifterna raderas helt från det medium där de lagras eller att de avidentifieras på ett sådant sätt att de inte är möjliga att koppla till en enskild individ eller går att återskapa.

När den ansvarige begär radering av uppgifter i en molntjänst signalerar det till biträdet att uppgifterna snarast ska utplånas eller avidentifieras. Enligt Datainspektionen är det acceptabelt att biträdets radering av personuppgifter görs med en viss fördröjning. Biträdet ska dock kunna förvissa den ansvarige om att uppgifterna raderas inom en viss angiven tid.

Underleverantörer

Av 31 § andra stycket personuppgiftslagen framgår det att den personuppgiftsansvarige ska förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att biträdet verkligen vidtar åtgärderna.

I Artikel 29-gruppens yttrande om molntjänster framgår att om ett personuppgiftsbiträde använder sig av underleverantörer är biträdet skyldigt att ge kunden tillgång till information om detta och beskriva

vilken typ av tjänst som underleverantören utför, vilka egenskaper nuvarande eller potentiella underleverantörer har, samt vilka garantier som uppställs för att dataskyddsdirektivet[11] kommer att följas.

Av yttrandet framgår också att ett personuppgiftsbiträde bara får lägga ut sin verksamhet på underentreprenörer om den personuppgiftsansvarige har lämnat sitt samtycke till detta. Den personuppgiftsansvarige kan lämna ett generellt samtycke när tjänsten börjar tillhandahållas.

Enligt Datainspektionen har personuppgiftsbiträdet en tydlig skyldighet att informera den ansvarige om eventuella planerade ändringar t.ex. att underentreprenörer läggs till eller tas bort. Den personuppgiftsansvarige ska hela tiden ha möjlighet att invända mot ändringarna eller säga upp avtalet. Det bör finnas en tydlig skyldighet för molnleverantören att ange alla underentreprenörer som anlitas.

Överföring av personuppgifter till tredje land

I personuppgiftslagen regleras överföring av personuppgifter till tredje land i 33–35 §§. Huvudregeln är att överföring är förbjuden till länder som inte har en adekvat nivå för skyddet av personuppgifter.

Överföring var tidigare tillåten till bolag i USA som är anslutna till Safe Harbor-principerna, eftersom EU-kommissionen hade beslutat att skyddsnivån i sådana fall skulle anses som adekvat. Systemet med Safe Harbor-principerna inbegriper ett antal principer angående skydd för personuppgifter vilka amerikanska företag frivilligt kan ansluta sig till.[12]

EU-domstolen har dock nyligen ogiltigförklarat kommissionens beslut.[13] I målet var frågan om en österrikisk medborgare som hade invänt mot att Facebook överför uppgifter om honom till USA. Som skäl för avgörandet anför EU-domstolen bl.a. följande. Systemet med Safe Harbor-principerna är endast tillämpligt för de amerikanska företag som anslutit sig till det. Förenta staternas myndigheter är

[11] 94/46/EG.

[12] Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, s. 7).

[13] EU-domstolens dom den 6 oktober 2015 i mål C-362/14, *Maximillian Schrems mot Data Protection Commissioner.*

inte själva bundna av det. Vidare har krav i fråga om den nationella säkerheten i Förenta staterna företräde framför Safe Harbor-systemet. Detta innebär att amerikanska företag är skyldiga att utan inskränkningar frångå systemets skyddsregler när de står i konflikt med sådana krav. Det amerikanska Safe Harbor-systemet möjliggör således ingrepp från de amerikanska myndigheternas sida i enskilda personers grundläggande rättigheter. I kommissionens beslut anges att det i Förenta staterna varken finns regler som syftar till att begränsa sådana eventuella ingrepp, eller något effektivt rättsligt skydd mot dessa.

Vidare påpekar EU-domstolen att en lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, kränker det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, eftersom en sådan möjlighet är en grundförutsättning för en rättsstat.

EU-domstolens dom innebär att en överföring av personuppgifter från ett EU-land till USA inte längre kan göras enbart med stöd av att det mottagande företaget i USA är anslutet till Safe Harbor-principerna.

Som en följd av detta, enades i februari 2016 EU-kommissionen och USA på ett övergripande plan om en ny ordning för transatlantiska dataflöden, kallad för ”sköld för skydd av privatlivet” (på engelska privacy shield). Artikel 29-gruppen har granskat dokumenten som ligger till grund för överenskommelsen och välkomnar de förbättringar som den innehåller jämfört med Safe Harbour-principerna. Artikel 29-gruppen hyser dock stora betänkligheter på en rad punkter beträffande både de kommersiella aspekterna och beträffande myndigheternas åtkomst, när uppgifter överförs med stöd av den nya överenskommelsen. Artikel 29-gruppen uppmanar därför Kommissionen att lösa de utestående problem med överenskommelsen och förbättra den så att den ger ett skydd som motsvarar EU:s dataskyddsregler.[14]

[14] *Statement of the Article 29 Working Party on the opinion on the EU-U.S. Privacy Shield*, den 13 April 2016.

Sekretess

Riksdagens ombudsmän (Justitieombudsmannen) har i ett beslut[15] den 9 september 2014 riktat allvarlig kritik mot vissa vårdgivare för att dessa ingått avtal om journalföring med ett företag, trots att detta inte varit förenligt med regelverket om sekretess inom hälso- och sjukvården.

I ärendet var förvisso inte frågan om någon molntjänst. Men eftersom beslutet rörde förhållandet mellan en personuppgiftsansvarig och ett personuppgiftsbiträde, har det betydelse även för personuppgiftansvarigas möjligheter att anlita molntjänstleverantörer för hantering av sekretessbelagda uppgifter.

Beslutet har gett upphov till en omfattande diskussion om hur det bör tolkas. Enligt Pensionsmyndigheten kan uppgifter från en myndighet, vilka som bedöms vara sekretessbelagda i förhållande till leverantören, inte hanteras för myndighetens räkning i en molntjänst, även om tystnadsplikt kan regleras i avtal. Men om myndigheten krypterar informationen innan den överlämnas till molntjänstleverantören ligger det enligt Pensionsmyndigheten nära till hands att uppgifterna inte kan anses röjda för leverantören och att sekretess inte ska hindrar ett utlämnande.[16]

Integritetskommittén konstaterar att rättsläget för närvarande måste betraktas som är oklart när det gäller tillämpningen av offentlighets- och sekretesslagen (2009:400) på hanteringen av sekretessbelagda uppgifter i molntjänster.

21.1.3 Kommitténs samlade bedömning av området

Molntjänster har vissa fördelar även ur ett integritetsskyddsperspektiv. Främst genom att säkerheten för personuppgifterna kan vara bättre hos en molntjänstleverantör än i den personuppgiftsansvariges egen it-miljö.

Det förutsätter dock att den personuppgiftsansvariga organisationen har gjort en grundlig risk- och sårbarhetsanalys och ställt krav på säkerheten som motsvarar uppgifternas känslighet. Redan i detta

[15] Dnr 3032-2011.

[16] *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015. Rapporten hänvisar i sin tur till E-delegationens förstudie om sekretess vid outsourcing, Fi 2009:01/2015/4, 2015-03-09.

led kan det finnas brister, exempelvis när den personuppgiftsansvarige felaktigt utgår från att det är molntjänstleverantören som ska göra en risk- och sårbarhetsanalys och sedan anpassa säkerhetsåtgärderna därefter. Resultatet kan då exempelvis bli att känsliga hälsouppgifter hanteras över internet med en säkerhet som är anpassad för uppgifter av helt annan, trivial natur. Det innebär i sin tur en risk för att de känsliga uppgifterna läcker ut och blir åtkomliga på internet. En härmed relaterad risk är att den personuppgiftsansvarige kunden gör underförstådda, men felaktiga, antaganden om att tjänsteleverantören genomför olika typer av säkerhetsaktiviteter, som exempelvis regelbundna tester med återläsning av säkerhetskopierad information, penetrationstester och skydd mot skadlig kod.[17]

De största integritetsrelaterade riskerna med molntjänster hänger emellertid ihop med förlusten av insyn och förlusten av kontroll som användningen av molntjänster i regel innebär.

Förlusten av insyn och kontroll innebär att det finns stora risker för att uppgifter kan komma att hanteras för biträdets eller underbiträdets egna ändamål Det finns också en risk för obehörig åtkomst hos leverantörer och underleverantörer. Leverantörer av molntjänster som är gratis eller mycket billiga grundar oftast sin verksamhet på att uppgifterna som hanteras har ett värde i sig. Uppgifterna kan exempelvis användas för att ta fram information om användarna. Efter sambearbetning med andra uppgifter går dessa att använda som annonsunderlag eller för att utveckla nya tjänster. Betalningen för molntjänsten utgörs då i praktiken av det värde som det innebär för leverantören att få åtkomst till uppgifterna. Det innebär att affärsmodellen i sig rymmer en inneboende drivkraft att använda kundernas uppgifter för egna ändamål och att dela med sig av dem till andra företag. I en rapport från år 2012 nämns just molnföretagens affärsmodeller som en av de största utmaningarna för användarnas integritet.[18]

Förlusten av insyn och kontroll innebär också att det finns stora risker för att uppgifterna hamnar hos underleverantörer som är okända för den personuppgiftsansvarige kunden. Det kan innebära att kunden i slutändan inte kan uppfylla sin skyldighet att se till att uppgifterna hanteras för rätt ändamål och på ett tillräckligt säkert sätt. Det finns likaså en risk att uppgifterna hamnar i länder där lag-

[17] Jfr *Molntjänster i staten, En ny generation av outsourcing*, Pensionsmyndigheten, 2015, s. 44.
[18] *Privacy in Cloud Computing*, 2012, International Telecommunication Union.

stiftningen ger ett otillräckligt skydd. Det kan exempelvis leda till att myndigheter och andra organisationer utanför EES lagligen kan få åtkomst till uppgifterna för ändamål och på ett sätt som inte hade varit lagligt i Sverige eller i något annat land inom EES.

Risken för detta uppstår så snart molntjänstleverantören är etablerad i ett tredje land, även om uppgifterna rent fysiskt hanteras på servrar i ett EES-land. Det visade sig i juli 2014 när en domstol i USA godkände ett föreläggande för Microsoft från rättsvårdande myndigheter i USA om att lämna ut uppgifter om en persons e-postkonto, utan att behöva begära rättshjälp från myndigheter i Irland.[19] Microsoft uppger sig ha fått liknande propåer från kinesiska myndigheter.

Många gånger presenteras molntjänster som färdigförpackade lösningar där den potentiella kunden bara har två valmöjligheter: att acceptera standardavtalen eller låta bli att använda tjänsten. Av Datainspektionens praxis framgår att standardavtal för molntjänster ofta ger leverantören goda möjligheter att hantera uppgifter för egna ändamål, även om sådana avtal strider mot 30 § personuppgiftslagen.

Personuppgiftslagen utgår från att det är den personuppgiftansvariga organisationen som bestämmer ändamål och medel för hanteringen av personuppgifter och som ger instruktioner till personuppgiftsbiträdet. Men när personuppgiftsbiträdet är en global molntjänstleverantör, blir förhållandet i praktiken vanligtvis det omvända, dvs. att biträdet bestämmer ändamål och medel som den personuppgiftsanvarige har att rätta sig efter om den vill använda sig av tjänsten.

Det kan vara mycket svårt för små aktörer, exempelvis mindre kommuner, att ha den kunskap som behövs för att bedöma vilka krav som gäller för att det ska vara möjligt att använda sig av en molntjänst på ett lagligt sätt. När kunskapen finns, kan det ändå vara mycket svårt att förmå en global molntjänstleverantör att anpassa sina avtalsvillkor till en liten kommuns krav.

Även om ett avtal med en molntjänstleverantör uppfyller kraven i personuppgiftslagen, är det i praktiken oftast omöjligt för den personuppgiftsanvarige att utöva någon reell kontroll av om uppgifterna verkligen hanteras i enlighet med avtalet.

[19] Avgörande den 31 juli 2014 av Chief U.S. District Judge Loretta A. Preska vid United States District Court, Southern District of New York, avgörandet har överklagats.

En annan risk med molntjänster kommer sig av att många av de populäraste tjänsterna är så billiga att det inte krävs någon upphandling eller ens en kontakt med den personuppgiftsansvariga organisationens it-avdelning innan tjänsten börjar användas. Tjänsterna är ofta enkla att använda och kan bidra till att effektivisera arbetet. Anställda kan därför välja att använda tjänsterna utan att organisationens ledning känner till det, eftersom det underlättar arbetsuppgifterna. Ansvaret enligt personuppgiftslagen för hur uppgifterna hanteras kan emellertid inte delegeras, utan ligger kvar på ledningen som helt saknar möjlighet att kontrollera en hantering vars förekomst i organisationen den inte ens känner till.

En komplikation som är specifik för Sverige, är det osäkra rättsläget när det gäller tillämpningen av offentlighets- och sekretesslagen på molntjänster, som uppstått efter det JO-beslut som nämns ovan i avsnittet om det skyddande regelverket.

När det gäller tillsyn var Datainspektionen i en jämförelse med andra EU-länder tidigt ute med att granska molntjänster och har sedan dess varit fortsatt aktiv i tillsynen av molntjänster. Tillsynsverksamheten har av allt att döma resulterat i att de stora molntjänstleverantörerna successivt blivit bättre på att anpassa sina standardavtal till kraven i personuppgiftslagen. Ännu har emellertid ingen hantering granskats som involverar känsliga personuppgifter, såsom molnbaserade journalsystem inom hälso- och sjukvården, försäkringsbranschen eller socialtjänsten.

Ur ett integritetsskyddsperspektiv utmärker sig särskilt publika molntjänster där flera leverantörer är inblandade. Vid användningen av dessa tjänster finns det en stor sannolikhet för att den personuppgiftsansvarige förlorar insyn och kontroll över uppgifterna. Den enskilde vars uppgifter flyttas till molnet har då förstås ännu mindre vetskap om eller möjlighet att påverka hur uppgifterna hanteras. Molntjänstleverantörerna får i praktiken ett större inflytande över hanteringen än den som bär det legala ansvaret gentemot den enskilde. Den personuppgiftsansvarige hamnar inte sällan i ett underläge i förhållande till leverantören, både i fråga om kompetens att bedöma hur tjänsterna fungerar och i fråga om vilka krav som bör ställas på tjänsterna. Publika molntjänster är vanligt förekommande och kan innehålla mycket stora informationsmängder. När en tjänst är gratis eller mycket billig, grundas erbjudandet många gånger på leverantörens vilja och möjlighet att använda uppgifterna i tjänsten

för egna ändamål. Sammantaget anser kommittén att publika molntjänster där flera leverantörer är inblandade, innebär en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att molntjänster bidrar till att effektivisera många verksamheter och möjliggöra nya tjänster. Molntjänster kan också ha fördelar ur ett integritetsskyddsperspektiv, främst genom att säkerheten för personuppgifterna kan vara bättre hos en molntjänstleverantör än i den personuppgiftsansvariges egen it-miljö.

21.2 Big data

Kommitténs bedömning: Big data för med sig allvarliga risker för den personliga integriteten.

21.2.1 Företeelsen

Vissa företeelser som brukar förknippas med big data har i korthet berörts i kapitel 12 om konsumentområdet.

Begreppet big data har ingen allmänt vedertagen definition, men brukar användas för att beteckna insamlingen och lagringen av så mycket data som möjligt av olika slag. Ibland inbegriper begreppet även den efterföljande analysen av uppgifterna, men denna kan även kallas för data mining. I denna text kommer big data användas för att även beteckna den efterföljande analysen.

En ibland citerad definition av big data är att det rör sig om informationstillgångar med stora volymer, som innehåller stora variationer och som kan hanteras mycket snabbt. Informationstillgångarna kräver kostnadseffektiva och innovativa sätt för bearbetning och analys och möjliggör förbättringar i fråga om kunskap, beslutsfattande och processautomatisering.[20]

Big data brukar därför ofta beskrivas med tre V:n, hämtade från engelskans volume (det vill säga mängden data), variety (många olika typer av data i olika format) och velocity (hastighet, eftersom tillgång till information och analyser ofta ges i realtid).

[20] Vår översättning av Gartner IT Glossary, Big data, http://www.gartner.com/it-glossary/big-data, hämtad 2015-10-04.

Det rör sig med andra ord om datamängder som är så stora och innehåller så många olika format, att det tidigare var svårt att hantera dem. Men med nya metoder är det i dag möjligt att hantera och analysera sådana datamängder.

Grunden till big data är de enorma mängder uppgifter som skapas och lagras i dag. Det är uppgifter från ett stort antal olika källor som exempelvis metadata från sökningar på internet, inköp med betalkort, sociala medier, sensorer i bilar eller mobiler, lokaliseringsdata från mobiltelefoner osv.

Det finns många olika beräkningar av hur mycket data ökar i världen.[21] Ett ofta återgivet exempel är att mänskligheten redan år 2010 dagligen skapade mer data än vad som sammanlagt någonsin hade skapats fram till år 2003. När sakernas internet utvecklas i framtiden, förväntas ökningstakten accelerera ytterligare (se kapitlet om konsumentområdet).

Det finns också uppskattningar som gör gällande att det under år 2015 kommer att skickas sammanlagt 76 exabytes data över internet, varvid en exabyte motsvarar ungefär 500 miljarder sidor text. Insamling och analys av alla dessa uppgifter är möjlig tack vare bl.a. drastiskt minskade kostnader för lagring. Att lagra ett petabyte data kostar i dag (år 2015) 100 000 USD per år, men kostade för bara fyra år sedan (år 2011) tio gånger mer, dvs. en miljon USD. Här har också utvecklingen av molntjänster spelat en stor roll, inte minst för mindre organisationers och privatpersoners möjligheter att lagra stora mängder uppgifter.

Det bakomliggande syftet med big data är att utnyttja dagens och morgondagens gigantiska datamängder för att leta efter mönster, sammanhang och förklaringar som inte var möjliga att upptäcka tidigare. Sådan kunskap är värdefull inte bara inom marknadsföring och försäljning, utan även för forskningen, sjukvården, brottsbekämpningen och inom samhällsplaneringen. Många gånger är det förutsägelser om framtiden som är av intresse – att i förväg få veta att en person snart kommer att göra något dyrt, som att skaffa barn, hus eller bil, eller något oönskat som att återfalla i brott, få problem med hälsan eller komma efter i skolan.

[21] De uppskattningar som nämns i det följande är hämtade från Bruce Schneier, *Data and Goliath*, W.W. Norton & Company, 2015, s. 18f.

Big data har medfört ett nytt sätt att se på data, där uppgifterna i sig får ett värde som grundar sig på hur det kan användas i framtiden.[22]

I sammanhanget är det emellertid viktigt att poängtera att långt ifrån alla användningsområden för big data involverar hantering av personuppgifter.

Ett belysande exempel på big data kan hämtas från hälso- och sjukvården. År 2014 rapporterades i media om ett amerikanskt vårdgivarföretag med långt gångna planer på att använda sig av big data i sin förebyggande verksamhet. I detta fall med hjälp av uppgifter om enskilda personers köpvanor. Vårdgivaren hade köpt sådana uppgifter från företag som specialiserar sig på att handla med uppgifter, s.k. datamäklare (eng. data brokers), vilka i sin tur samlat in uppgifter från offentliga register, från andra företags köpklubbar och från betalkortföretag. Tanken med detta är att läkarna på sikt ska kunna få varningar om patienter som köper produkter de inte borde eller på andra sätt utsätter sig för risker som inte är i linje med deras behandling eller hälsostatus.[23]

Ett annat exempel kan hämtas från brottsbekämpningen. Polisen i Los Angeles i USA använder sig i dag av matematiska modeller, ursprungligen utvecklade för att förutse jordskalv, i ett analysverktyg som kallas PredPol. Analysverktyget matas med lokal brottstatistik rörande bilstölder och inbrott, och med andra uppgifter som är av intresse för brottsbekämpningen. Med hjälp av PredPols analyser kan polisen förutse när ett visst brott kommer att begås, med vilken sannolikhet detta kommer att ske, och var på ett ungefär brottet kommer att begås, ner till områden så små som 150 kvadratmeter. Resultaten förs över till digitala kartor som polispatruller sedan kan använda sig av för att vara på plats redan innan brotten begås.[24]

Big data används i USA också för att avgöra hur stor risken är för återfall i brott för en viss person, i syfte att planera arbetet och resursfördelningen inom kriminalvården eller för att ta ställning till ansökningar om permission.[25]

---

[22] Norska Datatilsynets rapport *Big Data – personvernprinsipper under press*, september 2013.

[23] Shannon Pettypiece & Jordan Robertson, *Hospitals Are Mining Patients' Credit Card Data to Predict Who Will Get Sick*, daterad den 3 juli 2014 och publicerad på www.bloomberg.com (BloombergBusiness).

[24] Norska Datatilsynets rapport *Big Data – personvernprinsipper under press*, september 2013.

[25] Norska Datatilsynets rapport *Big Data – personvernprinsipper under press*, september 2013.

I Kina används big data för att på statligt initiativ skapa ett system för att värdera individer, i första hand för att bedöma deras kreditvärdighet, men i andra hand även för en rad andra ändamål, t.ex. vid visumansökningar, på dejtingsajter eller för att bedöma om vederbörande ska få adoptera ett husdjur. Bland uppgifter som används finns t.ex. uppgifter om sök- och köphistorik på nätet och om vilka personer individen har kopplingar till på sociala medier. Somliga tror att systemet i förlängningen kan komma att användas för att avgöra i vad mån den enskilde ska få sjukvård, utbildning, anställning och om han eller hon är att betrakta som en god medborgare i största allmänhet. Andra är mer skeptiska till möjligheterna att i Kina få till stånd ett fungerande kreditvärderingssystem baserat på uppgifter från nätet, eftersom det förekommer en hel del oriktiga uppgifter på nätet i Kina.[26]

Det är ingen tillfällighet att dessa exempel på tillämpningar av big data är hämtade från andra länder. I Sverige har användningen inte tagit samma fart, vilket bl.a. kan utläsas av publikationen *Big Data Analytics – A Research and Innovation Agenda for Sweden*.[27] Där sägs bl.a. att Sverige är i en bra position för att utnyttja big data, men att det återstår en hel del innan företag och myndigheter når sin fulla potential på området. Även utvecklingen av big data i Norge och Storbritannien, ligger en bit efter den amerikanska. Det framgår av de två rapporter från ländernas respektive dataskyddsmyndigheter vilka citeras i detta kapitel.

Det bör sägas att de stora datamängder som är aktuella här, inte nödvändigtvis behöver lagras i databaser. Detta i takt med att möjligheterna att snabbt hantera och analysera data i flöden (s.k. strömmande data) blivit allt bättre.[28]

[26] Charles Clover, *When Big data meets big brother,* publicerad på www.ft.com, den 19 januari 2016.

[27] Odaterad publikation från The Swedish Big Data Analytics Network och återgiven på bl.a. Vinnovas webbsida i oktober 2015.

[28] Lars Danielsson, *Strömmande data utmanar databasnormen*, publicerad på www.computersweden.idg.se, den 17 juli 2015.

21.2.2 Det skyddande regelverket

Personuppgiftslagens bestämmelser gäller för hanteringen av personuppgifter med hjälp av big data. Av särskild betydelse är i detta sammanhang personuppgiftslagens definition av personuppgifter samt lagens bestämmelser om ändamålsbegränsning, de andra grundläggande kraven på behandlingen och bestämmelserna om information och samtycke.

Personuppgift

För att personuppgiftslagen överhuvudtaget ska vara tillämplig, måste det röra sig om hantering av personuppgifter. Personuppgifter definieras i 3 § personuppgiftslagen som all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

För big data betyder det att helt anonyma uppgifter som först när de läggs ihop med andra anonyma data kan peka ut en enskild person, samtliga är att betrakta som personuppgifter enligt personuppgiftslagen.

Grundläggande krav

I 9 § personuppgiftslagen anges vissa grundläggande krav för att en hantering av uppgifter ska vara laglig.

Där anges bl.a. att den personuppgiftsansvarige ska se till att:

– personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål och att uppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (denna bestämmelse kallas ibland för ändamålsprincipen),
– de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
– inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,

– de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,
– alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och
– personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Av 9 § personuppgiftslagen framgår att de grundläggande kraven tar sin utgångspunkt i ändamålet med behandlingen. Ändamålet måste vara tillräckligt preciserat för att det överhuvudtaget ska vara meningsfullt att pröva hanteringen av uppgifterna och deras relevans, mängd, riktighet och bevarandetid. Om det inte går, är sannolikheten stor att ändamålet inte är tillräckligt preciserat.

Kraven i 9 § personuppgiftslagen innebär att varje hantering av personuppgifter i big data-sammanhang måste föregås av en tillräckligt preciserad avgränsning av ändamålet med hanteringen. Likaså får hanteringen inte omfatta fler uppgifter eller pågå under en längre tid, än vad som är nödvändigt i förhållande till det preciserade ändamålet.

Information och samtycke

Enligt huvudregeln i personuppgiftslagen får personuppgifter behandlas bara om den enskilda har fått information om behandlingen och därefter har lämnat sitt samtycke till den.

När huvudregeln är tillämplig innebär den att varje hantering av personuppgifter (dvs. inte bara analysen, utan även insamlingen och lagringen) också i big data-sammahang måste föregås av information (om bl.a. ändamålet med hanteringen) och av ett samtycke från den enskilde vars uppgifter ska hanteras.

Big data och dataskyddsprinciperna

Själva grundtankarna med big data innebär en utmaning för nämnda grundläggande krav i personuppgiftslagen, vilka härrör från de dataskyddsprinciper som lades fast i dataskyddsdirektivet. Ibland framförs t.o.m. att big data överhuvudtaget inte skulle gå att förena med dataskyddsprinciperna i direktivet.

Sådana påståenden har bemötts och problematiserats bl.a. av vissa dataskyddsmyndigheter. Exempelvis menar brittiska Commissioner's Office (ICO), att big data inte är ett ”spel med egna regler”, utan att dataskyddsprinciperna är tillräckligt flexibla för att kunna tillämpas även på big data, och att principerna inte omöjliggör företeelsen som sådan.[29]

21.2.3 Kommitténs samlade bedömning av området

Grundtankarna med big data framstår som svårförenliga med de allmänt vedertagna dataskyddsprinciper som kodifierats i dataskyddsdirektivet och som i svensk rätt återfinns i personuppgiftslagen. Frågan är därför i vad mån metoder och affärsmodeller som involverar big data överhuvudtaget kan anses som förenliga med lagstiftning som bygger på dessa dataskyddsprinciper.

Till att börja med bygger big data på en tro på att de flesta datamängder på något sätt kan komma till nytta i framtiden. Det betyder åtminstone på sikt att fler uppgifter kommer att samlas in än vad som noga taget skulle räcka för att tillgodose det egentliga och ursprungliga ändamålet med insamlingen och att dessa uppgifter inte heller kommer att gallras förrän det står helt klart att de inte länge behövs, om ens då. Det kommer sannolikt att leda till att det bildas allt större och detaljerade samlingar av uppgifter om enskilda.

En annan grundläggande tanke med big data är att nya och oväntade samband och förklaringar förväntas uppkomma när tidigare separata uppgiftssamlingar sambearbetas. Det fordrar att uppgifterna hanteras för helt nya ändamål som de enskilda i praktiken varken

[29] Rapport från Information Commissioner's Office *Big data and data protection*, version 1.0, juli 2014.

känner till, kanske inte ens hade kunnat föreställa sig och långt mindre har samtyckt till. Det kan leda till att enskilda fullständigt tappar kontrollen över hur och för vilka ändamål deras uppgifter hanteras.

Sambearbetning av stora mängder uppgifter i olika datasamlingar, som var för sig inte möjliggör identifiering av enskilda, kan leda till att det blir möjligt att identifiera enskilda som finns registrerade bland uppgifterna. På samma sätt blir det också allt svårare att åstadkomma en beständig anonymisering av datasamlingar, eftersom möjligheterna till återidentifiering blir allt bättre.

Vidare kommer ny kunskap om enskilda att uppstå när datasamlingar sambearbetas och okända samband och mönster framträder som har bäring på enskilda. Eftersom det kan röra sig om väldigt stora datamängder, kan resultatet innebära en mycket närgången kartläggning.

En annan risk består i de många möjliga felkällorna i big data. Det som utmärker uppgifterna i dessa sammanhang är volym och variation i typer av uppgifter, men kvalitet (i bemärkelsen riktighet och aktualitet) är sällan möjlig att upprätthålla eller ens att kontrollera. Det innebär en risk för att det skapas felaktiga uppgifter, och därmed också felaktiga slutsatser, om många personer.

En annan risk är att drivkraften att göra prognoser om enskilda med utgångspunkt i stora mängder historiska data, kan medföra en förstärkning och fördjupning av redan existerande fördomar och leda till diskriminering. Den risken blir ännu allvarligare om prognoserna används till att fatta automatiserade beslut som rör enskildas rättigheter och skyldigheter, utan att någon mänsklig beslutsfattare är inblandad.

Big data har ännu inte varit föremål för någon närmare granskning utifrån ett integritetsskyddsperspektiv i Sverige. Här har dataskyddsmyndigheterna i exempelvis Storbritannien och Norge kommit längre (se tidigare anförda rapporter från dessa länders respektive dataskyddsmyndighet).

Faktorer som i detta sammanhang är av betydelse för risken för den personliga integriteten, är att big data innebär att uppgifter hanteras för nya ändamål som inte är kända vid insamlingen. Det medför att den enskilde förlorar både kännedom om och inflytande över hur uppgifterna hanteras. Med big data blir det särskilt tydligt att per-

sonuppgifter betraktas som en handelsvara med ett högt kommersiellt värde. Det medför en avsevärt ökad risk för spridning av uppgifterna till parter som inte är kända för den enskilde.

Kommittén anser därför att big data för med sig en allvarlig risk för den personliga integriteten.

Samtidigt måste också beaktas att big data på ett genomgripande sätt kan komma att effektivisera och förbättra verksamheter i många delar av samhället.

21.3 Biometri

Kommitténs bedömning: Användningen av tekniker som involverar många och detaljerade biometriska uppgifter, innebär en påtaglig risk för den personliga integriteten.

21.3.1 Företeelsen

Biometri är samlingsnamnet på ett flertal olika tekniska lösningar som gör det möjligt att mäta kroppens egenskaper eller individers beteenden, och på så vis hitta särskiljande egenskaper hos olika individer.

Uppgifter om de egenskaper eller beteenden som mäts, s.k. biometriska uppgifter, kan definieras på följande sätt:

> Biologiska egenskaper, fysiologiska kännetecken, särdrag eller repeterbara handlingar där dessa kännetecken eller handlingar är både unika för individen och mätbara, även om de mönster som används i praktiken för att tekniskt mäta dessa bygger på ett visst mått av sannolikhet. [30]

Biometrisk teknik kan användas på i huvudsak två sätt:

1. *Verifikation*. Statistisk analys av insamlad biometrisk data från en individ gör det möjligt att med en hög sannolikhet verifiera att individen verkligen är den person som han eller hon utger sig för

[30] Artikel 29-gruppens yttrande 3/2012 om utvecklingen i fråga om biometrisk teknik, WP 193, antaget den 27 april 2012. Det finns även en standard för skyddet för biometriska uppgifter: ISO/IEC 24745:2011 Information technology – Security techniques – Biometric information protection.

att vara. I tekniska lösningar kallas detta förfarande ofta för autentisering. Ett exempel är den fingeravtrycksläsare som i dag finns i många mobiltelefoner och surfplattor, där jämförelse av biometriska data ersätter eller kompletterar en annan form av autentisering, t.ex. en pinkod. När rätt individ placerar sitt finger på fingeravtrycksavläsaren läses specifika delar av användarens fingeravtryck av. Dessa utgör sedan en inläst representation av individens finger vilken jämförs med det som finns lagrat i telefonen sedan tidigare. Om sannolikheten är tillräckligt hög att de är identiska så låses telefonen upp.[31]

2. *Identifikation*. Biometriska analysmetoder gör det möjligt att identifiera enskilda individer. Exempelvis har polisen länge använt fingeravtryck från brottsplatser på detta sätt. Efter att ha säkrat ett fingeravtryck från en oidentifierad brottsling jämförs det med de fingeravtryck som finns insamlade sedan tidigare, i hopp om att samma fingeravtryck ska finnas i samlingen och därmed göra det möjligt att knyta en specifik person till brottsplatsen.

Traditionellt sett har biometri handlat om fysiska egenskaper, exempelvis fingeravtryck. Men på senare tid går det också att använda beteenden som underlag för biometriska analyser. Ett sådant exempel är tangentbordsrytm. Sättet att skriva på ett tangentbord skiljer sig åt mellan olika individer och kan därmed fungera som dynamisk data lämpad för statistisk analys. Detta för att hitta särskiljande mönster i tangentbordsrytmen mellan olika individer.

Ett annat exempel är s.k. signaturbiometri. Det är en beteendebaserad biometrisk teknik för att mäta en persons beteende uttryckt genom dynamiken i utförandet av namnteckningen. Traditionell signaturigenkänning baseras på analys av statiska eller geometriska egenskaper hos den visuella bilden av signaturen (hur signaturen ser ut). Signaturbiometri handlar i stället om en analys av de dynamiska egenskaperna hos signaturen (hur signaturen gjordes). Typiska dynamiska egenskaper som mäts med ett system för signaturbiometri (t.ex. en digitalplatta) är trycket, skrivvinkeln, pennans hastighet och acceleration, formningen av bokstäver, penndragens riktning och andra unika dynamiska kännetecken. Det finns utrustning för

[31] iOS Security—White Paper, september 2015. https://www.apple.com/business/docs/ iOS_Security_Guide.pdf, s. 8, hämtat 2016-04-20.

signaturigenkänning som genomför verifieringen genom en kombinerad analys av både statiska egenskaper (den visuella bilden) och dynamiska egenskaper (tryck, vinkel, hastighet osv.) hos en signatur.[32]

Biometriska system lagrar uppgifter om vissa s.k. extraherade egenskaper hos den ursprungliga informationen, t.ex. från ett fingeravtryck. Dessa utgörs av de särdrag som systemets algoritmer lokaliserat i bilden.

Det finns en rad olika biometriska tekniker som i dag används inom olika områden. Till dessa mätbara egenskaper eller beteenden hör bl.a. följande:

- Fingeravtryck
- Ansikten
- Regnbågshinna
- Näthinna
- Ögonbotten (retina)
- Gångstil
- DNA
- Hand- och fingergeometri
- Kroppslukt
- Röst
- Tangentbordsrytm
- EEG (hjärnans elektriska aktivitet)
- Hjärtrytm
- Venmönster, dvs. mönster i människors blodådror.

I takt med att tekniken för biometri blir bättre, billigare och mindre, används den i allt fler sammanhang. Ett exempel med stor spridning är att alla pass som i dag utfärdas i EU-länderna är försedda med ett chip där innehavarens fingeravtryck finns lagrat.

[32] Artikel 29-gruppens yttrande 3/2012 om utvecklingen i fråga om biometrisk teknik, WP 193, antaget den 27 april 2012.

Biometrisk teknik som använder sig av DNA förekommer i dagsläget främst inom brottsbekämpningen. Ett exempel på hur biometriska uppgifter om DNA kan användas för internationellt samarbete inom brottsbekämpningen, är det så kallade Prümfördraget, vilket numera är en del av EU:s lagstiftning. Det ger medlemsländerna en viss rätt att få tillgång till bl.a. nationella DNA-databaser och fingeravtrycksdatabaser i samband med brottsbekämpning. Sverige började i november 2013 att arbeta med sökningar enligt Prümfördraget gentemot Nederländerna och gentemot Finland i mars 2014. Det innebär att DNA-profiler från alla svenska spår som inte ger en nationell träff mot någon person samt DNA-profiler från alla svenska misstänkta och dömda personer, automatiskt söks mot dessa länders DNA-register.[33]

Riskerna med att använda sig av uppgifter om DNA har resulterat i att det finns särskild lagstiftning om s.k. genetisk integritet: lagen (2006:351) om genetisk integritet, m.m. Enligt lagens förarbeten ska genetisk integritet ses som en del av den personliga integriteten – den kan sägas vara helheten av en individs eller arts arv, som inte får eller bör kränkas. Det motiveras med att det bl.a. är den genetiska koden som avgör den biologiska människans särart och identitet. Den genetiska integriteten kan kränkas på flera sätt t.ex. genom manipulation, genom att forskning bedrivs utan adekvat informerat samtycke, genom att testresultat läcker ut till arbetsgivare och försäkringsbolag eller genom kommersialisering.[34]

Avläsning och mätning av regnbågshinnan används tillsammans med fingeravtrycksavläsning på kanadensiska flygplatser för att kontrollera att endast behörig personal får tillträde till vissa delar av flygplatserna.[35]

Fingeravtrycksavläsning förekommer bl.a. på arbetsplatser. Datainspektionen granskade år 2010 fingeravtrycksavläsning som användes av ett företag för närvarokontroller och tidrapportering av anställda.[36] Företaget i fråga hade uppgett att man haft problem med att anställda hade rapporterat in närvaro för varandra, vilket angavs som ett av skälen till att fingeravtrycksavläsning infördes. Datainspektio-

[33] Polisens webbsida om Prümfördraget, http://nfc.polisen.se/om-SKL/internationellt-samarbete/prumfordraget/ hämtad 2016-03-29.
[34] Prop. 2005/06:64, Genetisk integritet m.m., s. 35.
[35] Transport Canadas websida http://www.tc.gc.ca/eng/aviationsecurity/page-168.htm, hämtad den 2016-03-29.
[36] Datainspektionens beslut den 12 november 2010 i dnr 1765-2009.

nen kom fram till att användningen av fingeravtrycksavläsning var tillåten i detta fall, om de anställda samtyckte till det. För att det skulle vara fråga om giltiga samtycken enligt personuppgiftslagen, krävdes enligt Datainspektionen dels att de anställda hade fått information om behandlingen, dels att de anställda erbjöds en alternativ metod till den biometriska behandlingen och att de inte fick utsättas för någon direkt eller indirekt påtryckning att välja det alternativ som innebar behandling av biometriska uppgifter.

I ett tidigare ärende om fingeravtrycksavläsning hos Datainspektionen, var frågan om användning av tekniken för att se till att endast elever som hade betalat för skolmaten kunde hämta ut tallrikar från en tallriksautomat.[37] Datainspektionen menade att hanteringen av elevernas fingeravtyck var otillåten, eftersom den kunde uppfattas som ett intrång i elevernas personliga integritet, och eftersom kontrollen i stället kunde genomföras på ett för eleverna mindre integritetskänsligt sätt, utan att deras fingrar lästes av. Datainspektionens beslut ändrades dock av Regeringsrätten, som fastslog att användningen av fingeravtrycksavläsning i tallriksautomaten kunde vara tillåten under förutsättning att samtycke från eleverna inhämtades.[38]

Det bör avslutningsvis nämnas att ett av målen för utvecklingsarbetet inom biometrisk teknik, är att kunna samla in biometriska uppgifter på avstånd eller i rörelse, utan att den enskilde behöver samarbeta eller agera.

21.3.2 Det skyddande regelverket

Vilken lagstiftning som är tillämplig på användningen av biometrisk teknik, beror på inom vilket område tekniken används.

Ofta är personuppgiftslagen tillämplig. I den lagen är det särskilt vissa bestämmelser som är av betydelse i sammanhanget. Dels bestämmelserna om att uppgifter inte får behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet med insamlingen, dels bestämmelserna om att uppgifterna ska vara riktiga och att inte fler personuppgifter behandlas än som är nödvändigt.

[37] Datainspektionens beslut den 13 januari 2005 i dnr 1601-2004.
[38] RÅ 2008 ref. 83.

Vidare är bestämmelserna om den lagliga grunden för behandlingen av betydelse, t.ex. om det finns ett reellt (dvs. informerat och frivilligt) samtycke, om behandlingen i stället kan grundas på ett avtal med den registrerade personen eller om behandlingen är tillåten med anledning av ett berättigat intresse hos den personuppgiftsansvarige (dvs. efter en intresseavvägning mellan den registrerades och den ansvariges olika intressen).

Slutligen är också personuppgiftslagens bestämmelser om säkerhet av betydelse, dvs. de bestämmelser som kräver att uppgifter skyddas genom lämpliga tekniska och organisatoriska åtgärder.

I sin faktabroschyr Personuppgifter i arbetslivet (reviderad i juni 2015) skriver Datainspektionen att det krävs tungt vägande skäl för att en arbetsgivare ska få behandla biometriska uppgifter om arbetstagarna med stöd av en intresseavvägning. Rent allmänt vägs åtgärder som betingas av säkerhetsskäl tyngre än åtgärder som betingas av företagsekonomiska effektivitetsskäl.

För att arbetsgivaren ska få använda biometri för närvaro- och tidsrapportering krävs enligt Datainspektionen normalt att arbetstagarna samtycker till behandlingen. För att samtycket ska vara giltigt måste arbetstagaren ha ett verkligt fritt val och senare kunna ta tillbaka sitt samtycke utan att det medför några nackdelar för honom eller henne. Det innebär bland annat att arbetstagaren, liksom när det gäller positioneringsteknik, måste erbjudas en alternativ metod, exempelvis att logga in genom användarnamn och lösenord, samt att han eller hon inte får utsättas för någon direkt eller indirekt påtryckning att välja det alternativ som innebär behandling av biometriska uppgifter.

21.3.3 Kommitténs samlade bedömning av området

Användningen av biometriska tekniker innebär flera olika risker för den personliga integriteten. Vissa av de risker som nämns här, behandlas utförligt i Artikel 29-gruppens yttrande från år 2012 om utvecklingen i fråga om biometrisk teknik.[39]

[39] Artikel 29-gruppens yttrande 3/2012 om utvecklingen i fråga om biometrisk teknik, WP 193, antaget den 27 april 2012.

En risk är att biometriska uppgifter behandlas för nya ändamål som är oförenliga med de ändamål för vilka uppgifterna ursprungligen samlades in. Exempelvis kan biometriska uppgifter om gångstil och ansikte användas inte bara för att identifiera enskilda, utan också för att hitta oönskade beteenden eller särskilda behov hos enskilda.

En annan risk är att fler biometriska uppgifter hanteras än vad som behövs för ändamålet, t.ex. att hela fingeravtryck samlas in och lagras när det i själva verket hade varit tillräckligt att bara hantera vissa mätpunkter från fingeravtrycket. Detsamma kan inträffa när uppgifter om DNA inte bara möjliggör identifiering, utan även avslöjar något om den registrerades hälsotillstånd, sjukdomsbenägenhet eller etniska ursprung.

Ytterligare en risk är att biometriska uppgifter inte skyddas tillräckligt och som en följd av detta blir tillgängliga för personer som kan använda uppgifterna för exempelvis identitetsstöld.

Det finns också en risk för att biometriska uppgifter kan användas utan att den enskilde känner till det eller lämnar sitt samtycke, t.ex. vid publicering av bilder på nätet eller i sociala medier där det finns särskild programvara för ansiktsigenkänning.

Det finns slutligen också en risk för överutnyttjande av biometri när tekniken blir billigare, enklare och därmed mer lättillgänglig. Alla sammanhang kräver inte den höga precision som biometri kan erbjuda.

En ökad användning av olika biometriska tekniker i samhället, riskerar att göra det mycket svårt att någonstans i det offentliga rummet kunna vara helt anonym, när kameror och annan utrustning i omvärlden kan läsa av och identifiera den enskildes kropp eller personliga beteende och koppla ihop de biometriska uppgifterna med uppgifter från andra datakällor.

Sammantaget anser kommittén att användningen av tekniker som involverar många och detaljerade biometriska uppgifter, innebär en påtaglig risk för den personliga integriteten.

Samtidigt måste beaktas att biometriska tekniker kan medföra stora fördelar t.ex. genom att bidra till att höja säkerhetsnivån vid åtkomst- eller tillträdeskontroller och genom att göra identifierings- och autentiseringsförfaranden säkrare genom kombination med andra metoder, men också enkla, snabba och bekväma för den enskilde.

DEL IV

Övrigt

22 Informationssäkerhet och integritet

Kommitténs bedömning: Det finns starka indikationer på väsentliga brister i informationssäkerheten hos offentliga organisationer, t.ex. i organisationer med mycket omfattande personuppgiftsbehandlingar som i kommunerna. I kapitel 11 om e-förvaltning gör kommittén bedömningen att dessa brister måste sägas medföra en allvarlig risk för den personliga integriteten.

22.1 Inledning

Det finns en ökad medvetenhet om att de landvinningar som blivit resultatet av den digitala revolutionen också lett till nya problem när det gäller den personliga integriteten. Om den fulla potentialen av digitaliseringen ska kunna utnyttjas inom bland annat handel, vård och omsorg och den offentliga förvaltningens tjänster måste skyddet av den personliga integriteten kunna hanteras på ett sådant sätt att den enskilde känner tillit till och är villig att använda de tjänster som erbjuds. Det skydd av personuppgifter som bidrar till den nödvändiga tilliten bygger på ett systematiskt informationssäkerhetsarbete. Den enskilde behöver själv vidta åtgärder för att minska risken för kränkning av den egna integriteten, men ett stort ansvar för skyddet av personuppgifter vilar också på de offentliga och privata organisationer som hanterar uppgifterna. Skydd för den personliga integriteten är nära sammanlänkad med informationssäkerhet.

22.2 Informationssäkerhet som område

Nästan allt vi gör i dag kretsar kring information; att lämna, att ta emot, att bearbeta och förädla. Därför måste information skyddas så att den alltid finns när den behövs (tillgänglighet), att den är korrekt och inte har manipulerats eller blivit förstörd (riktighet) och att endast de som har behörighet har åtkomst (konfidentialitet). Dessa krav kompletteras ibland även med en eller flera andra egenskaper, såsom spårbarhet, oavvislighet, ansvarighet, autenticitet och auktorisation.[1] I den s.k. NISU-utredningen[2] definieras informationssäkerhet på följande sätt:

> Informationssäkerhet innebär en strävan att skydda information så att den alltid finns när den behövs (tillgänglighet), att det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Informationssäkerhet omfattar såväl administrativa som tekniska åtgärder för att skydda information.

Informationssäkerhet enligt den modell som tillämpas bland annat i statliga myndigheter utgår från 27000-serien inom The International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) standardsystem. Det innebär att en organisations ledning ska inrätta ett ledningssystem som säkerställer att organisationens information hanteras på ett korrekt och lagenligt sätt.

Systematiken utgår från ledningens styrning och ställer krav på att en verksamhet ska vidta åtgärder som står i proportion till de risker som den är utsatt för. Detta brukar uttryckas som att verksamheten ska ha ett riskbaserat förhållningssätt.

För att kunna hantera riskerna krävs att verksamheten genomför en riskbedömning som är ändamålsenlig och verksamhetsanpassad. Verksamheten ska identifiera, förstå och bedöma riskerna för händelser som innebär till exempel förlust eller röjande av skyddsvärd information.

[1] Standard. Terminologi för informationssäkerhet, SIS-TR 50:2015.
[2] NISU 2014 betänkande *Informations- och cybersäkerhet i Sverige*, SOU 2015:23.

Det innebär i sin tur att en rad aktiviteter ska planeras, genomföras, utvärderas och kontinuerligt förbättras inom informationssäkerhetsområdet. Grundläggande är att analysera verksamhetens behov av skydd för olika informationstillgångar med utgångspunkt i de risker som omger verksamhetens informationshantering. Detta förutsätter att organisationen har god kontroll över vilka informationstillgångar som man har ansvar för och är beroende av.

Ledningens styrning ska beskrivas i ett ledningssystem för informationssäkerhet (LIS), som ska dokumenteras på ett för organisationen lämpligt sätt. En central punkt i ett sådant ledningssystem är att klarlägga ansvar och roller för informationssäkerhet. En beskrivning av hur riskanalys, informationsklassning, hur incident- och kontinuitetshantering ska genomföras, liksom hur säkerhetsaspekter ska ingå vid utveckling och upphandling av it-lösningar, är andra viktiga delar i ett ledningssystem för informationssäkerhet.

22.3 Det skyddande regelverket

I 31 § personuppgiftslagen (1998:204) ställs krav på informationssäkerhetsåtgärder. Där framgår att den personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,

b) vad det skulle kosta att genomföra åtgärderna,

c) de särskilda risker som finns med behandlingen av personuppgifterna, och

d) hur pass känsliga de behandlade personuppgifterna är.

Det är denna bestämmelse som ger Datainspektionen rätten att genom tillsyn ta ställning till den tekniska och organisatoriska säkerheten i samband med personuppgiftsbehandling.

På telekomområdet ställs krav på säkerhetsåtgärder enligt 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation för att säkerställa att uppgifter som behandlas i samband med tillhandhållande av

en allmänt tillgänglig elektronisk kommunikationstjänst. Motsvarande krav ställs även på den som tillhandahåller ett allmänt kommunikationsnät.

I den ovannämnda NISU-utredningen ingår ett kapitel om den rättsliga regleringen på informationssäkerhetsområdet. Utredningen delar upp regleringen i; övergripande lagstiftning med relevans för informationssäkerhetsområdet, reglering av säkerhetsskydd, krisberedskap och informationssäkerhetsarbete, specifik reglering av brottsbekämpande och underrättelsemyndigheters arbete på området samt nämner slutligen brottsbalken.

I den övergripande lagstiftningen inbegrips tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400). Hanteringen av allmänna handlingar ställer krav på informationssäkerhetens samtliga aspekter (konfidentialitet, riktighet, tillgänglighet och spårbarhet). Även personuppgiftslagen, registerförfattningar, arkivlagen och lagen om elektronisk kommunikation hör till denna kategori.

Reglering av säkerhetsskydd, krisberedskap och informationssäkerhet finns i säkerhetsskyddslagen (1996:627), som innehåller bestämmelser angående skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet. Säkerhetsskyddet ska även förebygga terrorism. Säkerhetsskyddet har ett avgränsat syfte och ställer även krav på specifika informationssäkerhetsåtgärder som beskrivs i regleringen. Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap reglerar statliga myndigheters arbete med krisberedskap och ansluter också till vad som föreskrivs i lagen (1992:1403) om totalförsvar och höjd beredskap i fråga om civil verksamhet. I förordningen (2016:1053) om totalförsvar och höjd beredskap finns bestämmelser om myndigheters ansvar att i sin verksamhet beakta och planera för totalförsvarets krav. Enligt 19 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska varje myndighet omge sin informationshantering med lämpligt skydd så att myndigheten kan utföra sin verksamhet på ett tillfredsställande sätt.

Myndigheten för samhällsskydd och beredskap har regeringens uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. Myndigheten har föreskriftsrätt inom informations-

säkerhetsområdet. Myndigheten har utfärdat föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1). Myndigheten har även utfärdat föreskrifter gällande kryptoberedskap (MSBFS 2009:11), obligatorisk it-incidentrapportering (MSBFS 2016:2) och krav på risk- och sårbarhetsanalyser i statliga myndigheter (MSBFS 2015:3) samt landsting (MSBFS 2015:4) och kommuner (MSBFS 2015:5).

Ett antal av ovanstående regelverk gäller även för den privata sektorn där även annan reglering med krav på informationssäkerhet tillkommer som exempelvis i bokföringslagen (1999:1078).

Utöver detta finns indirekta krav på informationssäkerhetsåtgärder i syfte att skydda hanteringen av personuppgifter i annan lagstiftning som kommer behandlas under andra kapitel i utredningen. Krav kan även finnas i branschregelverk och andra typer av självreglerande överenskommelser i olika branscher.

22.4 Lägesbild över informationssäkerheten i Sverige

En väl fungerande informationssäkerhet är en viktig grund för ett väl fungerande integritetsskydd. En bedömning av nivån på informationssäkerheten i svenska offentliga och privata organisationer är därför intressant, eftersom den kan ge en uppfattning om vilka möjligheter organisationerna har att skydda de personuppgifter som de hanterar.

För att ge en bild av informationssäkerhetsläget behövs tre huvudsakliga komponenter; inventering av skyddsvärda informationstillgångar (till exempel databaser med personuppgifter), bedömning av risker och beskrivning av nivån på vidtagna skyddsåtgärder. För svenska förhållanden finns ingen sammanställd lägesbild av informationssäkerheten. Uppgifter får därför hämtas från flera källor.

När det gäller hot och risker gör myndigheter med särskilt ansvar för informationssäkerhet, som Myndigheten för samhällsskydd och beredskap, Polisen och Försvarsmakten, en löpande rapportering till regeringen. I sin roll som samordnande ska Myndigheten för samhällsskydd och beredskap rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället. Myndigheten ska även årligen lämna en rapport till regeringen med en sammanställ-

ning av de it-incidenter som rapporterats in enligt 20 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Även Post- och telestyrelsens årliga risk- och sårbarhetsanalys över sitt ansvarsområde ger viktigt underlag för bedömningen av hot och risker.[3]

Flera av dessa myndigheter går också samman och publicerar trendrapporter över den aktuella situationen.[4] Ytterligare en rapport har tagits fram av Myndighetens för samhällsskydd och beredskap för att samla erfarenheter från ett antal större it-incidenter.[5] Det finns ingen publikation som ger en samlad bild av hoten mot svensk informationsbehandling. Viss information finns att hämta i den europeiska informationssäkerhetsmyndighetens rapport Threat Landscape 2015.[6] Rapporten är främst inriktad på antagonistiska hot där bedömningen är att hoten har blivit allt allvarligare. Till detta kommer sådana risker som inte uppstår ur antagonistiska hot, som t.ex. hård- och mjukvarufel och bristande rutiner för exempelvis åtkomst- och behörighetshantering.

Det finns ett antal rapporter som kan ge en uppfattning om hur väl utvecklat det informationssäkerhetsarbete är som syftar till att reducera hot och risker. Framför allt är det offentliga verksamheter som har blivit granskade, medan underlaget för den privata sektorn är betydligt mer begränsat.

De statliga myndigheternas informationssäkerhet har granskats i två relativt aktuella rapporter, från Riksrevisionen respektive Myndigheten för samhällsskydd och beredskap.[7] Rapporterna visar att det finns ett antal brister både i statens styrning av informationssäkerhetsarbetet och hur de enskilda myndigheterna de facto bedriver detta arbete. Sammanfattande observationer i Riksrevisionens granskning är att:

- Regeringen inte utövar en effektiv styrning av informationssäkerheten i den civila statsförvaltningen

[3] 2015-års risk- och sårbarhetsanalys för PTS och dess ansvarsområden, PTS dnr 15-4951.
[4] Informationssäkerhet – trender 2015, publiceringsnummer MSB 799.
[5] It- och informationssäkerhet i Sverige Erfarenheter och reflektioner från några större it-incidenter under 2012–2014, Publikationsnummer MSB721.
[6] ENISA Threat Landscape 2015.
[7] RiR 2014:23 Informationssäkerheten i den civila statsförvaltningen och En bild av myndigheternas informationssäkerhetsarbete 2014, Publikationsnummer MSB740.

- Regeringens stöd- och tillsynsmyndigheter endast delvis har vidtagit nödvändiga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas.

Avsaknaden av lägesbild är som framgår en av de brister som Riksrevisionen betonar i sin granskningsrapport.

Av rapporten från Myndighetens för samhällsskydd och beredskap framgår att många myndigheter saknar väsentliga förutsättningar för ett systematiskt informationssäkerhetsarbete trots att myndighetens föreskrifter trädde i kraft den 1 februari 2010. År 2015 genomförde myndigheten en liknande undersökning hos de svenska kommunerna. Resultatet av denna blev sämre än för de statliga myndigheterna på flera punkter.[8]

Myndigheten för samhällsskydd och beredskap har också regeringens uppdrag att i samverkan med berörda aktörer redovisa en nationell bedömning av samhällets förmågor, risker, sårbarheter samt identifierade och genomförda åtgärder avseende krisberedskapen. I bedömningen ska även informationssäkerhet beaktas. Myndigheten gjorde år 2016 bedömningen att risker gällande informationssäkerhet i otillräcklig utsträckning identifieras och analyseras

En slutsats är att hot relaterade till informationssäkerhet kan sägas vara i ständig tillväxt medan verksamheternas skydd av den information de hanterar inte utvecklas i samma takt – i vart fall inte inom den offentliga förvaltningen, som är den sektor som varit föremål för djupare granskning. Rapporterna över svenska förhållanden visar på en bristande nationell styrning och att de myndigheter som har till uppgift att ge stöd till andra organisationer inte löst uppdraget på ett tillfredsställande sätt.

22.5 Informationssäkerhet och integritet

22.5.1 Relationen mellan informationssäkerhet och integritet

Sambandet mellan informationssäkerhet och integritet är flerdimensionellt. Målet med informationssäkerhet är att skapa och upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet för in-

[8] En bild av kommunernas informationssäkerhetsarbete 2015, Publikationsnummer MSB943.

formationen vilket inkluderar att skydda människors personliga integritet. Samtidigt kan vi konstatera att åtgärder som vidtas för att förbättra informationssäkerheten också kan motverka integritetsintresset. Ett exempel på detta är tekniska övervakningsfunktioner.

Det systematiska informationssäkerhetsarbetet är riskbaserat och bygger, som beskrivits ovan, på analyser av risker som kan identifieras beträffande informationshanteringen i en verksamhet. En hypotetisk situation kan illustrera sambandet mellan informationssäkerhet och integritet.

Myndigheten A ska utveckla en tjänst där medborgare via ett webbgränssnitt ska rapportera in uppgifter om sina personliga förhållanden för att en ersättning ska betalas ut. Vid den riskanalys och informationsklassning som genomförs initialt i utvecklingsprojektet identifieras ett antal risker som kan uppstå och som kan påverka den enskildes integritet, som till exempel:

- Uppgifterna som lämnas är inte aktuella vilket kan leda till att meddelanden skickas till fel adress (riktighet, konfidentialitet)
- Mer information hämtas in än vad som är nödvändigt i förhållande till det syfte som är formulerat för tjänsten (riktighet)
- Fler handläggare än vad som är nödvändigt för att lösa specificerade arbetsuppgifter har åtkomst till uppgifterna (tillgänglighet)
- Det är inte möjligt att i efterhand kontrollera vilka handläggare som varit inne i tjänsten och tagit del av uppgifterna kring en viss person (spårbarhet).
- Systemet dit uppgifterna ska lämnas är underdimensionerat och blir otillgängligt under längre perioder (tillgänglighet)
- En grupp hackare tar sig in och får åtkomst till informationen för att sälja den vidare (konfidentialitet)

De risker som identifierats och värderats kan därefter reduceras med organisatoriska och tekniska åtgärder. Personuppgiftslagen är tillämplig eller kan vara tillämplig vid samtliga ovan nämnda exempel.

Det systematiska informationssäkerhetsarbetet erbjuder alltså både verktyg för att identifiera och analysera risker och för att vidta olika typer av skyddsåtgärder, i syfte att reducera riskerna för den personliga integriteten. Till riskerna hör att personuppgifter används

i annat syfte än de inhämtats för, att samtycke inte inhämtas för en viss behandling av personuppgifter eller att behandlingen av personuppgifter inte görs på ett sådant sätt att den önskade transparensen uppstår. Till de skyddande åtgärderna hör det som brukar betecknas som Privacy enhancing technologies (PET) som syftar till att reducera risker för den personliga integriteten i it-miljöer.[9] Det kan till exempel handla om åtgärder för att minimera inhämtandet av personuppgifter eller möjligheter för pseudonymisering.[10]

Insatserna för att utveckla och förvalta en god informationssäkerhet respektive skydda den personliga integriteten överlappar varandra. I vissa fall kan det ligga en intressekonflikt mellan å ena sidan informationssäkerhetsarbetet och å andra sidan den personliga integriteten som exempelvis när det gäller vissa typer av loggning (spårbarhet). I informationssäkerhetsintresset kan då ligga att skapa och bevara tekniska loggar för att kunna gå tillbaka och se när en händelse inträffade, en transaktion genomfördes eller motsvarande, medan loggarna sett ur ett integritetsperspektiv kan utgöra ett problem, om de till exempel används för andra ändamål, inte gallras eller inte skyddas tillräckligt.

22.5.2 Risker för integriteten ur ett informationssäkerhetsperspektiv

Personlig integritet förutsätter att individer har en möjlighet att skapa och kontrollera en privat sfär. Den privata sfären är inte bara fysisk utan består också av information om den enskildes levnadsförhållanden. Att kunna skydda information som går att härleda till enskilda individer, att säkerställa att den är korrekt samt att ha en spårbarhet som möjliggör transparens är viktigt för att kunna skapa ett

[9] Ett förslag på definition är följande: Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system. (van Blarkom, Borking & Olk 2003).

[10] Mer om tekniska åtgärder finns att läsa i rapporten ”Integritetsskyddande teknik” som togs fram av Kirei på utredningens uppdrag (bilaga 4) och i Marcus Bylund *Personlig integritet på nätet* (Falun 2013).

adekvat skydd av individernas personliga integritet. En ökad risk för kränkning av den personliga integriteten är i hög grad relaterad till brister i informationssäkerhetsarbetet.[11]

Den ökande mängden information som samlas in och hanteras, de många olika möjligheterna att hantera information och snabbheten i hur den överförs har medfört en hastigt förändrad riskbild för den personliga integriteten och ställer krav på informationssäkerhetsarbetet. Riskerna uppstår vid inhämtningen, vid överföringen, vid hanteringen, vid lagringen och vid presentationen av information som innehåller personuppgifter. Med tanke på det värde som personuppgifter betingar i olika hänseenden finns det många intressenter förutom de aktörer som samlar och hanterar personuppgifter i ett primärt syfte. Det kan vara myndigheter med uppdrag att genomföra övervakning i brottsbekämpande syfte eller annan uppföljande verksamheter, eller det kan vara försäkringsbolag som samlar uppgifter i syfte att begränsa försäkringsskyddet för en person. Personuppgifter är även en allt mer väsentlig komponent i kriminella verksamheter av olika slag.

Inhämtning av personuppgifter görs i allt fler former, som exempelvis via molntjänster, appar, e-tjänster, sakernas internet (Internet of Things), biometri, Radio Frequency Identification (RFID), positioneringssystem, drönare, övervakningskameror, s.k. kakor och genom olika övervakningsfunktioner inom välfärdsteknologin. Inhämtning av personuppgifter görs såväl öppet, med samtycke från den enskilde och med legitima syften som även i rent kriminell verksamhet. Det förekommer t.ex. att enskilda luras att fylla i uppgifter som sedan används för att genomföra identitetsstöld. Användningen av s.k. spionprogramvara som samlar in individens digitala spår på nätet, som sedan kan användas för bland annat direkt marknadsföring är också vanligt förekommande.

En utgångspunkt för att skydda den personliga integriteten är att inta ett minimalistiskt förhållningssätt – det vill säga att ingen aktör eller medarbetare ska ha tillgång till mer information om individer än vad som krävs för att lösa den aktuella arbetsuppgiften. Sett ur ett informationssäkerhetsperspektiv måste en avvägning göras mellan tillgänglighet, riktighet och konfidentialitet då behörighetssystem utformas.

[11] Marcus Bylund *Personlig integritet på nätet* (Falun 2013), Torbjörn Tännsjö Privatliv (Sweden 2010) och Tobias Pulls *Preserving privacy in transparency logging* (Karlstad 2015).

Förhållningssättet ställs dock ofta i motsats till kravet på effektivitet eftersom det kan hävdas att det är rationellt att så många medarbetare som möjligt ska kunna utföra olika arbetsuppgifter. Hos en it-leverantör är det exempelvis en fördel att slippa begränsa antalet systemadministratörer som kan gå in och genomföra rutinåtgärder i en applikation som hanterar en kunds information.

Intresset av att kunna använda personalen på ett så flexibelt sätt som möjligt är inte begränsat till privata aktörer utan gäller även i offentlig sektor. Det gör att det kan förekomma en alltför generös behörighetstilldelning även hos myndigheter. Ett nyligen uppdagat exempel på detta var då det i Försäkringskassans utredning av fusk med assistansersättning visade sig att större delen av myndighetens personal hade tillgång till personuppgifter om funktionshindrade.[12] Förutom att känsliga personuppgifter på ett regelvidrigt sätt lämnats ut till vårdföretagare, hade de assistansberättigades rätt till personlig integritet åsidosatts genom att myndigheten gett de anställda alltför vida behörigheter. Kraven på konfidentialitet hade med andra ord satts för lågt i detta fall.

Frågor som hur länge uppgifter lagras, om och hur de sammanställs med andra uppgifter, om de överförs till andra aktörer och var de lagras kan vara svåra att få svar på. Den i dag mycket spridda användningen av appar kan tjäna som exempel för några osäkerhetsfaktorer. En populär form av appar där känsliga personuppgifter registreras av användaren själv är hälsoappar som ska ge stöd för träning, dieter eller behandlingar. Vid en nyligen genomförd genomgång av några av de populäraste hälsoapparna genomförd av en norsk konsumentorganisation visade det sig att det råder oklara avtalsförhållanden om hur den insamlade informationen om individer kan delas. Dessutom gallras informationen i många fall inte även om användaren säger upp kontot utan ligger kvar hos leverantören.[13] Eftersom uppgifter om hälsa och träning är värdefulla ur ett marknadsföringsperspektiv är sannolikheten hög för att de kan säljas vidare i ett sådant syfte.

[12] Katarina Helmerson, *Personal på Försäkringskassan misstänks för brott*, http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=6377256, hämtad den 22 maj 2016

[13] Pressmeddelande på Sveriges konsumenters webbplats den 23 februari 2016, http://sverigeskonsumenter.se/nyheter-press/pressmeddelanden/stora-integritetsbrister-i-halso-och-traningsappar/

När personuppgifter samlas in i stor skala skapas också attraktiva mål för olika typer av antagonistiska aktiviteter. Det kan handla om att stater försöker skaffa sig uppgifter som kan understödja deras nationella intressen, men även om kriminella grupper som använder uppgifterna själva eller säljer dem vidare. En gråzon mellan kriminalitet och legitima affärsintressen kan uppstå vid försäljningen av personuppgifter. De antagonistiska hoten kan ta olika former. Hackning är kanske den mest uppenbara, det vill säga att aktörerna tar sig in i it-system och därefter kan få tillgång till personuppgifter. Detta kan även göras genom användning av skadlig kod med mera. En av de största attackerna internationellt var intrånget år 2015 i en dejtingsajt, Ashley Madison, som i marknadsföringen framhöll möjligheten att hitta någon för en utomäktenskaplig affär. Intrånget innebar att personuppgifter och kontokortsuppgifter för uppskattningsvis 39 miljoner människor stals av en grupp som uppgav att de gjort intrånget eftersom man ansåg otrohet vara moraliskt förkastligt. Det kan ifrågasättas om detta var det verkliga skälet, men händelsen är intressant eftersom det visar att intrång kan genomföras inom en stor spännvidd av aktörer. Liknande intrång där miljontals användarnamn, e-postadresser, lösenord och kontokortsuppgifter stulits har även genomförts hos t.ex. programvaruleverantören Adobe och på spel- och underhållningssiter som Sony, Heroes of Newerth och Gamigo.

Hälso- och sjukvården är den bransch där flest känsliga personuppgifter hanteras vilket också i takt med digitaliseringen innebär ökade risker för integritetsintrång. Fenomenet med ökat antal hacker-attacker mot sjukvården har hittills varit mest uppmärksammat i USA där miljontals patienter fått sina journaler stulna av hackare.[14] I vissa fall har journaluppgifterna blivit stulna hos försäkringsbolag som fått dessa som underlag för försäkringar. I Sverige uppmärksammas oftare interna hot mot patientuppgifter än externa, t.ex. när sjukvårdspersonal har skaffat sig obehörig åtkomst till jour-

[14] Se exempelvis *Cyberattack Surge: 100M medical records hacked in 2015, officials say*, publicerat den 23 december 2015 på www.foxnews.com, Jonas Hartelius och Lita Tibbling Grahn, *Facit 2015: 100 miljoner intrång i digitala journaler i USA*, debattartikel publicerad den 15 januari 2016 på www.lakartidningen.se, Kate Conger, *4.5 million patient records were accessed in UCLA hack*, publicerad den 20 juli 2015 på www.digitaltrends.com, Jeremy Baker, *Nearly four million medical records hacked*, publicerad den 3 augusti 2015 på www.kens5.com

nalinformation.[15] Bakgrunden till detta kan sannolikt vara att det i svensk sjukvård är vanligt med omfattande behörigheter för personalen där den tekniska och logiska begränsningen av åtkomst till patienters journaler är svag liksom uppföljningen.[16]

En form av hot som blivit allt vanligare är att aktören ”kidnappar” informationen med hjälp av skadlig kod, t.ex. genom att kryptera den och därefter begär en lösensumma för att informationsägaren ska tillbaka sina uppgifter. Ransomware, som den här typen av programvara kallas, har mer storskaligt använts bland annat riktad mot amerikansk sjukvård men även svenska kommuner[17] och andra organisationer har blivit drabbade. Huvudsyftet vid användningen av ransomware är inte att ta del av informationen, men genomförandet innebär ändå att den kriminella aktören har tillgång till den.

Skatteverket drabbades av en av de större nationella it-attackerna då folkbokföringsregistret hackades år 2012. Genom angreppet kopierades tusentals skyddade personuppgifter. Registret, som hanterades av it-företaget Logica, omgavs av en undermålig säkerhet vilket möjliggjorde intrånget. En orsak till att den personliga integriteten allvarligt påverkades för ett mycket stort antal människor var de oklara ansvarsförhållandena mellan Skatteverket och de underleverantörer som hanterade registret. Vid den polisutredningen som följde intrånget framkom att inga konkreta säkerhetskrav ställts av Skatteverket.

Oklara ansvarsförhållanden i samband med att flera parter samverkar kring informationshantering är ett stort riskområde. Det kan handla om att relevanta säkerhetskrav inte ställs eller inte följs upp, att informationsmängder sammanställs från olika källor och bildar nya register eller att distinkta kvalitetskrav inte formuleras vilket kan leda till inkorrekta personuppgifter. Vid användning av outsourcing och molntjänster kan det vara svårt för den personuppgiftsansvarige att följa företagsstrukturerna på den internationella marknaden och ha kontroll över den faktiska lagringen av personuppgifterna. Det kan vara en svår uppgift för många organisationer att utöva en effek-

[15] Se exempelvis Michael Lövtrup, *Dataintrång kan leda till att legitimationen återkallas*, Läkartidningen. 2015;112:DDPR och Sanna Rayman, 177 integritetsbrott är 177 för många, publicerad den 6 maj 2013 på www.svd.se

[16] MSB rapport. Uppföljning av informationssäkerhet i vården. Vårdgivarnas rapportering av kontroller, risker och incidenter.

[17] Jakob Eidenskog, *Kommunen utpressas efter dataintrång,* http://www.svt.se/nyheter/lokalt/vast/kommunen-utpressad-efter-dataintrang, hämtad den 22 maj 2016.

tiv kontroll över att kraven i personuppgiftslagen och de egna säkerhetskraven följs i varje led. Upphandling av och samverkan om it-relaterade lösningar har därför blivit en allt viktigare informationssäkerhetsfråga.[18]

Större it-incidenter kan utgöra stora risker även om de inte har ett antagonistiskt ursprung. I vissa fall kan själva återställningsarbetet efter en tillgänglighetsincident innebära att organisationer genomför extraordinära åtgärder som innebär att personuppgifter hanteras på ett annat sätt än det normala. Exempel på detta uppmärksammades vid den så kallade Tieto-incidenten år 2011.[19]

22.5.3 Ett europeiskt perspektiv på informationssäkerhet och integritet

Det starka sambandet mellan informationssäkerhet och integritet har uppmärksammats även på europeisk nivå. Kraven i dataskyddsdirektivet bygger på att det finns en tydlig styrning av informationshanteringen så att personuppgifter omges med ett tillräckligt skydd. Förutom skydd mot obehörig åtkomst ställer direktivet krav på bland annat riktighet och spårbarhet

The European Union Agency for Network and Information Security (ENISA), som har uppdraget att samordna EU:s arbete med nät- och informationssäkerhet, har tagit flera initiativ på området. Bland annat tog man år 2014 fram en guide som beskriver hur skyddet av integritet kan utformas i it-relaterade tjänster och system. ENISA har här utvidgat begreppet för konceptet till Privacy and Data Protection by Design och guiden ger stöd för hur organisationer kan samordna integritetsaspekterna med det övriga informationssäkerhetsarbetet.

Organisation for Economic Co-operation and Development (OECD) har ett liknande angreppssätt. OECD ser informationssäkerhet som en nödvändig förutsättning för att kunna realisera de gemensamma lösningar för ekonomi, handel, hälsa och andra samhällsfunktioner som eftersträvas. Informationssäkerhet och integritet har ett nära samband för OECD vilket bland annat demonstreras av

[18] Vägledning – informationssäkerhet vid upphandling, publiceringsnummer MSB 555.
[19] Detta beskrivs i MSB:s rapport Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, publikationsnummer MSB 367-12.

att en gemensam arbetsgrupp för informationssäkerhet och integritet har skapats.[20] Från Sveriges sida har Post- och telestyrelsen deltagit i arbetet. OECD har också lyft fram integritetsfrågorna som en viktig framgångsfaktor för den ekonomiska utvecklingen. År 2013 kom en ny version av The OECD Privacy Framework där organisationen framhåller att man under decennier spelat en viktig roll i främjandet av integritet som ett fundamentalt värde och som ett villkor för ett fritt flöde av personuppgifter över landsgränser.

Även The International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) arbetar med dessa frågor. En standard med inriktning på personlig integritet har tagits fram, ISO/IEC 29100 Privacy Framework. Standarden ska ses som ett komplement till övriga säkerhetsstandarder som ISO/IEC 27000 om ledningssystem för informationssäkerhet med syftet att på ett tydligt sätt föra in integritetsaspekterna i det övriga säkerhetsarbetet. Ett viktigt bidrag är de elva principer vars syfte är att stödja en organisation i att skapa it-lösningar och informationshantering som värnar den enskildes integritet.[21] Informationssäkerhet definieras som en egen princip samtidigt som ett systematiskt informationssäkerhetsarbete lyfts fram som en förutsättning för att kunna genomföra flertalet av de övriga principerna.

22.5.4 Inriktning för informationssäkerheten i Sverige ur ett integritetsperspektiv

Under det senaste decenniet har ett antal initiativ tagits för att förbättra samhällets informationssäkerhet. Ursprunget till dagens nationella informationssäkerhetsarbete går i hög grad att finna i den proposition om samhällets säkerhet och beredskap som regeringen lade fram år 2001.[22] I propositionen ingår en strategi för informationssäkerhet i samhället och skydd av samhällsviktiga it-beroende system. Strategin har en mycket tydlig inriktning på statens intresse av att skydda samhällsviktiga verksamheter och då inte minst mot

[20] Working Party on Information Security and Privacy in the Digital Economy – WPSPDE.

[21] Principer: Consent and choice, Purpose legitimacy and specification, Collection limitation, Data minimization, Use, retention and disclosure limitation, Accuracy and quality, Openness, transparency and notice, Individual participation and access, Accountability, Information security och Privacy compliance.

[22] Regeringens proposition *Samhällets säkerhet och beredskap, p*rop. 2001/02:158.

antagonistiska attacker. Värnet av demokratiska värden och den personliga integriteten ingår också och har funnits med som en målbild i efterföljande utredningar. Den närmast följande utredningen kallades InfoSäkutredningen.[23] En väsentlig del av utredningens uppdrag var att utveckla strategin som lanserats i propositionen från år 2001, vilket gjordes genom att utredningen föreslog tio strategiska inriktningar för informationssäkerhetsarbetet En av dessa var: *skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet*.

Utredningens strategiska målbild har med små förändringar kommit att leva kvar under ett antal år. I realiteten kan dock inte utredningen sägas ha gjort integritet till en viktig del av den svenska informationssäkerhetspolitiken med tanke på att man inte presenterade några konkreta förslag för att förbättra den enskildes integritetsskydd. Den personliga integriteten, när den omnämns, beskrivs i de flesta fall som en instrumentell förutsättning för att uppnå målen i den svenska it-politiken med en ökad användning av digitala lösningar. För att medborgarna ska kunna känna sig trygga och vilja använda exempelvis myndigheters e-tjänster måste ett skydd av den personliga integriteten kunna utlovas. Personuppgiftslagen och Datainspektionens uppdrag beskrivs men utredningen gör inga ansatser att integrera det konkreta skyddet av den personliga integriteten i den svenska informationssäkerhetspolitik som man föreslår. I utredningens slutbetänkande[24] nämns inte heller skyddet av den personliga integriteten som ett statligt åtagande.

Utredningen ger en illustration av ett problem som därefter återkommit i många andra sammanhang på grund av att begreppet integritet används i två olika betydelser. Den första betydelsen är den innebörd som begreppet har i exempelvis i personuppgiftslagen. Den andra betydelsen har sitt ursprung i bland annat EU:s definition av informationssäkerhet, där användningen av begreppet är synonymt med det engelska *integrity*. Begreppet betyder i detta sammanhang företeelsen att en databas, ett nätverk, ett system alternativt en informationsmängd är skyddad från oavsiktlig förändring eller förlust av information. De två olika betydelserna används omväxlande i utredningen. Utredningens förslag om en nationell strategi föranledde att regeringen år 2007 gav Krisberedskapsmyndigheten) i uppdrag att ta

[23] InfoSäkutredningens huvudbetänkande *Säker information Förslag till informationssäkerhetspolitik.* SOU 2005:42.
[24] *Informationssäkerhetspolitik – Organisatoriska konsekvenser,* SOU 2005:71.

fram en nationell handlingsplan för samhällets informationssäkerhet. Handlingsplanen presenterades år 2008 och innehöll bland annat ett förslag om uppdatering av strategin, ett arbete som den nybildade Myndigheten för samhällsskydd och beredskap fick uppdraget att leda.

År 2009 lade regeringen fram en skrivelse om samhällets krisberedskap som även innehöll ett längre avsnitt om informationssäkerhet och uppdateringen av den nationella strategin. Informationssäkerhetens betydelse för samhället beskrivs på följande sätt:

> Informationssäkerhet handlar om att säkra informationssystem i syfte att värna olika värden i samhället såsom demokrati, personlig integritet, tillväxt samt ekonomisk och politisk stabilitet.[25]

Samtidigt framgår det att inriktningen fortfarande i hög grad är skyddet av nationella intressen:

> I dag betraktas informationssäkerhet av de flesta länder som en stor nationell utmaning och anses också vara av strategisk, utrikespolitisk och säkerhetspolitisk betydelse.

Vad som mer än tidigare lyftes fram är att informationssäkerhet är en del av samhällets krisberedskap.

Värnet av den personliga integriteten finns med som ett av sex mål för det strategiska informationssäkerhetsarbetet. Det kan därför tyckas inkonsekvent att Datainspektionen inte ingår i den grupp av myndigheter som ska delta i den centrala samordningen av samhällets informationssäkerhet. I regeringsskrivelsen uttalas följande:

> Det övergripande ansvaret på nationell nivå är i dag uppdelat på ett antal myndigheter bl.a. Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt, Post- och telestyrelsen, Rikskriminalpolisen, Säkerhetspolisen, Försvarsmakten och Försvarets materielverk.

Det är också endast de uppräknade myndigheterna som ingår i Samverkansgruppen för informationssäkerhet (Samfi).

[25] Regeringens skrivelse 2009/10:124, Samhällets krisberedskap – stärkt samverkan för ökad säkerhet.

År 2014 tillsatte regeringen en ny utredning med uppgift att analysera *övergripande och strategiska åtgärder för hantering och överföring av information i elektroniska kommunikationsnät och it-system* (den tidigare nämnda NISU 2014). Utredarens uppdrag var bland annat att föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system, samt föreslå övergripande mål för samhällets informationssäkerhetsarbete. De förslag, som lades, handlar om det kollektiva skyddet för information som staten ska kunna erbjuda. I de delar utredningens förslag skulle kunna påverka den enskildes personliga integritet föreslår utredningen ytterligare utredningsåtgärder för att väga in sådana aspekter.[26]

För närvarande pågår arbete i regeringskansliet med en ny strategi för samhällets informationssäkerhet.

22.6 Tillsyn och informationssäkerhet

Datainspektionen är i första hand en tillsynsmyndighet som genom sin verksamhet ska bidra till att behandlingen av personuppgifter inte medför otillbörligt intrång i enskildas personliga integritet. Enligt personuppgiftslagen ska den som är personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Den personuppgiftsansvarige bör alltså bedriva ett systematiskt informationssäkerhetsarbete. Till tekniska åtgärder räknas saker som brandväggar, krypteringsfunktioner och virusskydd, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation och rutiner, instruktioner och policyer.

Den underliggande modellen för säkerhetsarbete som Datainspektionen rekommenderar i sina allmänna råd[27] bygger på samma principer som ett ledningssystem för informationssäkerhet (LIS) enligt ISO/IEC 27001 och 27002, som är de standarder som föreskrivs för statliga myndigheter i MSBFS 2009:10. Den personuppgiftsansvarige ska kartlägga hotbilden (riskanalys), sätta upp mätbara mål för säkerhetsarbetet, fastställa en policy, skapa en organisation för

[26] SOU 2015:23.
[27] Datainspektionens allmänna råd om säkerhet för personuppgifter.

säkerhetsarbetet, vidta skyddsåtgärder samt följa upp att målen nås. Säkerhetsåtgärderna som föreslås är också desamma som i standarden: loggning, lösenordshantering, fysiskt skydd för utrustning m.m.

22.7 Kommitténs samlade bedömning av området

Den enskilda individen har i de flesta fall liten möjlighet att påverka hur de egna personuppgifterna hanteras. Kunskapen om vilka säkerhetsåtgärder som den enskilde själv kan vidta för detta ändamål (förutom att avstå helt från olika tjänster) är begränsad och fokuserar oftast på åtgärder som att hantera sina lösenord på ett bra sätt. Ett tungt ansvar vilar därmed på privata företag och organisationer och kanske särskilt på offentliga myndigheter när det gäller att skapa ett gott integritetsskydd.

Det finns starka indikationer på väsentliga brister i informationssäkerheten hos offentliga organisationer, t.ex. i organisationer med mycket omfattande personuppgiftsbehandlingar som i kommunerna. I kapitel 11 om e-förvaltning gör kommittén bedömningen att dessa brister måste sägas medföra en allvarlig risk för den personliga integriteten.

Dessvärre finns det inte några aktuella undersökningar som beskriver förhållandena på den privata sektorn. Kommittén har därför inte underlag för att göra en generell bedömning över den delen av samhället. Kommittén anser att frånvaron av sådant underlag är en allvarlig brist i sig.

En konsekvens av bristerna i informationssäkerheten är att möjligheten att upprätthålla ett väl fungerande skydd för den personliga integriteten blir försvårad. Med tanke på att ett antal av de skyddsåtgärder som rekommenderas av bland annat OECD och ENISA, som exempelvis anonymisering, pseudonymisering och kryptering, är svåra att införa inom vissa samhällssektorer, finns ett behov av samordning på nationell nivå, t.ex. när det gäller standarder och normer. Det finns även ett behov av att i högre grad integrera arbetet med att skydda den personliga integriteten med det traditionella informationssäkerhetsarbetet.

23 Vilket skydd erbjuder samhället den enskilde?

Kommitténs bedömning: Den fysiska eller juridiska person som gör ett otillbörligt intrång i någon annans personliga integritet, löper liten risk att råka ut för någon sanktion, vare sig av tillsynsmyndigheterna, genom någon ersättningsskyldighet eller något straff. Den som drabbas av detta intrång får inte en ersättning som motsvarar den upplevda kränkningen. Sanktionssystemet har på så sätt inte den kompensatoriska och preventiva effekt som är önskvärd.

23.1 Inledning

Vår utredning visar att en enskild person utsätts för en mängd olika integritetsrisker i det dagliga livet. Risker som uppstår i kontakten med andra privatpersoner, med företag och med myndigheter. Det finns lagstiftning, branschöverenskommelser och etiska regler som syftar till att minska de risker som finns i samband med hantering av personuppgifter. Men vilka skyddsmekanismer finns det i övrigt mot integritetskränkningar? Finns det verkningsfull tillsyn, ändamålsenliga möjligheter till ersättning och tillräckliga sanktioner?

I kapitel 6 om *Det grundläggande rättsliga skyddet* och då särskilt avsnittet om sanktioner (6.8) finns en genomgång av de rättsliga regler som syftar till att bestraffa, kompensera och förhindra integritetskränkande handlingar genom tillsyn, ersättning och straff.

Andra utredningar med angränsade uppdrag

En särskild utredare[1] har i januari 2016 lämnat en översyn av det straffrättsliga skyddet för enskildas personliga integritet, särskilt när det gäller hot och andra kränkningar från andra enskilda. Utredaren har i betänkandet bl.a. anfört att skyddet för den personliga integriteten bör utformas utifrån att varje människa förtjänar respekt och att bemötas med värdighet.[2] I betänkandet föreslås en ny straffbestämmelse om olaga integritetsintrång, som innebär ett straffansvar för den som gör intrång i någon annans privatliv genom att sprida bild eller annan uppgift på ett sätt som syftar till att medföra kännbar skada för den som uppgiften rör. Utredaren föreslår också en rad förtydliganden av befintliga straffbestämmelser i brottsbalken till skydd för den personliga integriteten. Dessutom föreslår utredningen att rätten till brottsskadeersättning ska utvidgas till vissa ärekränkningsbrott.

Tillsyn är ett annat medel som samhället erbjuder för att bevaka att regler följs som syftar till att stödja den personliga integriteten. Ansvaret för tillsyn på integritetsområdet ligger i dag på flera olika myndigheter. Regeringen beslutade i december 2014 att tillsätta en utredning[3] om hur skyddet för den personliga integriteten kan förstärkas genom att i högre grad samla tillsynen över personuppgiftsbehandling hos en myndighet. I syfte att stärka skyddet för den personliga integriteten ska utredaren överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet.

Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten har alltså lämnat förslag avseende det straffrättsliga skyddet främst vid spridning av uppgifter på nätet och med inriktning på kränkningar mellan enskilda. Utredningen om tillsynen över den personliga integriteten[4] lämnar inom kort förslag avseende tillsynens organisering. Därtill kommer Mediegrundlagsutredningen[5] som bl.a. ska analysera om skyddet för den personliga

[1] Dir. 2014:74.
[2] Utredningens om ett modernt och straffrättsligt skydd för den personliga interiteten betänkande *Integritet och straffskydd*, SOU 2016:7 s. 180.
[3] Dir 2014:164.
[4] Ju 2015:02.
[5] Ju 2014:17.

integriteten i databaser med utgivningsbevis är tillräckligt.[6]Vidare ska Utredningen om dataskyddsförordningen[7] bl.a. analysera vilka bestämmelser om administrativa sanktionsavgifter och andra sanktioner som Sverige behöver eller bör införa med anledning av den nyligen beslutade allmänna dataskyddsförordningen som ska ersätta dataskyddsdirektivet och personuppgiftslagen (se kapitel 6 om det grundläggande rättsliga skyddet).[8] *Integritetskommitténs uppdrag*
Vårt uppdrag är att kartlägga faktiska och potentiella risker som kan påverka enskilda individer från integritetssynpunkt. Vår genomgång visar att behandlingen av personuppgifter ökar kraftigt inom i stort sett samtliga samhällsområden. Därmed kan vi även rent generellt påstå att risken för otillbörliga intrång i den personliga integriteten ökat påtagligt. Det allmänna har ett ansvar för att skydda enskildas privatliv och integritet. Kommittén vill därför undersöka om samhället erbjuder ett skydd som är verkningsfullt i samband med de risker som är förknippade med användning av modern informationsteknik.

De skyddsmekanismer som vi ska behandla i detta kapitel är:

- Tillsyn
- Ekonomisk ersättning
- Straffrättsliga sanktioner

[6] Dir. 2014:97.
[7] JU 2016:04.
[8] Dir. 2016:15.

23.2 Tillsyn

23.2.1 På vilket sätt kan tillsyn ge ett skydd?

Tillsynens syfte är att skydda medborgarnas gemensamma intressen särskilt inom områden som omfattar den enskilde individens rättigheter, trygghet och säkerhet.[9] Tillsyn är en administrativ process genom vilken offentliga organ vakar över följsamheten till demokratiskt fattade beslut.

Genom tillsynen har lagstiftaren gett vissa myndigheter en rätt – och en skyldighet – att vid behov ingripa mot förhållanden, handlingar, processer m.m. vilka strider mot medborgarnas intressen som de har reglerats i lag. Tillsynen spelar på detta sätt en viktig roll för medborgarnas förtroende för såväl staten som för andra vitala funktioner i samhället.[10]

När det gäller skyddet för den personliga integriteten kan tillsynen sägas vara särskilt viktig. Dels introduceras i en mycket snabb takt nya företeelser, som det finns anledning att fortlöpande bedöma ur ett rättsligt perspektiv. Dels är regelverket tämligen oprecist och avsiktligt allmänt hållet. Det är därför ofta först när tillsynsmyndigheten har bedömt en företeelse, som leverantörer och användare får någon ledning. Resultatet från tillsynen kan sedan användas i tillsynsmyndighetens utåtriktade och proaktiva arbete för att sprida kunskap.

Datainspektionen

Det finns flera myndigheter som har i uppdrag att vaka över att de regler följs som syftar till att skydda den enskildes rätt till en skyddad sfär. I kapitel 6 finns en översiktlig beskrivning av tillsynsmyndigheterna och deras uppdrag. När det gäller tillsynen över behandling av personuppgifter är det Datainspektionen som har det övergripande ansvaret. Datainspektionen ska genom sin tillsynsverksamhet bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet.

[9] Tillsynsutredningens betänkande *Statlig tillsyn – Granskning på medborgarnas uppdrag*, SOU 2002:14, s. 138.
[10] SOU 2002:14, s. 139.

Post- och telestyrelsen

Det är Post- och telestyrelsen som ansvarar för tillsyn enligt lagen (2003:389) om elektronisk kommunikation och dess integritetsskyddsregler. Lagens regler om integritet gäller behandling av uppgifter som har samband med elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Dessa regler handlar bland annat om vad operatörerna får göra med uppgifter om sina kunder och uppgifter som är nödvändiga för att kommunikationen ska kunna förmedlas. Reglerna har sitt ursprung i det bakomliggande EU-direktivet om integritet och elektronisk kommunikation (2002/58/EC).

Konsumentverket och Konsumentombudsmannen

Även Konsumentverket har en roll när det gäller tillsyn över intrång i enskilda konsumenters personliga integritet. Konsumentverket utövar tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden. Konsumentombudsmannen kan utfärda förelägganden och inleda rättsprocesser mot företag som bryter mot lagen om avtalsvillkor i konsumentförhållanden.

Övriga tillsynsmyndigheter

Riksdagens ombudsmän (Justitieombudsmannen) är en myndighet under riksdagen och en del av riksdagens kontrollmakt. Justitieombudsmannen har bl.a. i uppgift att se till att myndigheter och domstolar följer regeringsformens bestämmelser om opartiskhet och saklighet samt att den offentliga verksamheten inte gör intrång i medborgarnas grundläggande fri- och rättigheter.

Justitiekanslern utövar tillsyn över myndigheter och deras tjänstemän. Tillsynen syftar till att kontrollera att lagar och andra författningar följs och är främst inriktad på att upptäcka systematiska fel i den offentliga verksamheten.

Länsstyrelserna utöver tillsyn när det gäller kameraövervakning av platser dit allmänheten har tillträde. Det finns även sektorsspecifika myndigheter som utövar tillsyn, t.ex. *Inspektionen för vård och omsorg, Säkerhets- och integritetsskyddsnämnden samt Statens inspektion för försvarsunderrättelseverksamheten*.

23.2.2 Fungerar tillsynen?

Datainspektionens tillsyn

Datainspektionen är i dag en myndighet med ca 45 årsarbetskrafter. Uppdraget är omfattande. Myndigheten har tillsynsansvar över i stort sett all personuppgiftsbehandling i hela samhället.

När det gäller klagomål från människor som upplever att de blivit kränkta genom att deras personuppgifter har publicerats på internet kan Datainspektionen sällan agera. Till exempel kan de anmälda webbplatserna eller publiceringarna träffas av något av undantagen i personuppgiftslagen (1998:204), som innebär att lagen inte ska tillämpas. Vidare kan det vara svårt eller omöjligt för Datainspektionen att utreda vem som t.ex. står bakom en viss publicering på internet. Enligt vad Datainspektionen uppger i årsredovisningen för 2015 är de klagomål som gäller internetkränkningar ofta mycket resurskrävande, eftersom det ofta är fråga om svåra överväganden där det gäller att bedöma var gränsen går i förhållande till den grundlagsskyddade yttrandefriheten. Datainspektionen har inte resurser att utreda alla inkommande klagomål, utan prioriterar ärenden där myndigheten kan åstadkomma största möjliga nytta, ärenden som innebär tydliga överträdelser av personuppgiftslagen och sådana som kan leda till att ny praxis skapas. Eftersom Datainspektionens tillsynsmöjligheter på internetområdet i vissa fall är begränsade är informationsspridning och samverkan med andra myndigheter, i arbetet som handlar om kränkningar på internet, en viktig del av Datainspektionens arbete. Datainspektionen har under 2015, efter klagomål från enskilda, inlett ett större tillsynsärende mot ett företag som tillhandahåller en sökmotor på internet, avseende den så kallade rätten att bli glömd.

Av Datainspektionens årsredovisning för 2015 framgår att allt mer resurser läggs på att svara på remisser och delningar. Antalet avgivna remissyttranden har ökat från 117 för 2014 till 143 år 2015.

Samtidigt har antalet påbörjade tillsynsärenden minskat från 214 ärenden år 2013 till 85 ärenden år 2014 och enbart 53 ärenden år 2015. Kostnaderna för att svara på remisser har sedan 2013 ökat med ungefär tre miljoner samtidigt som kostnaderna för tillsynsärenden minskat med omkring två miljoner.

Enligt uppgift från Datainspektionen har myndigheten under de fem senaste åren gjort 18 polisanmälningar avseende brott mot personuppgiftslagen.

Datainspektionens befogenheter

Bestämmelserna om Datainspektionens befogenheter återfinns i huvudsak i 43–47 §§ personuppgiftslagen och reglerar sådant som exempelvis följande.

- Myndighetens rätt att för sin tillsyn få tillgång till personuppgifter och tillträde till lokaler (43 §).
- Myndighetens möjlighet att vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifterna på annat sätt än genom att lagra dem (44 §).
- Myndighetens möjlighet att föreskriva vite om den personuppgiftsansvarige inte frivilligt följer att beslut om säkerhetsåtgärder enligt 32 § personuppgiftslagen (45 §).

Datainspektionen har alltså möjlighet att vid vite föreskriva den personuppgiftsansvarige att vidta åtgärder för att rätta eventuella brister som myndigheten funnit i sin tillsyn. Ett sådant vite kan dock enligt 45 § personuppgiftslagen endast föreskrivas för att förmå den personuppgiftsansvarige att vidta säkerhetsåtgärder. Någon annan möjlighet att med vite förena ett föreläggande om att uppnå ett visst resultat eller att vidta åtgärder som rör annat än säkerhet, finns således inte.

Datainspektionen har i en skrivelse till Regeringen i december 2011[11] framfört att det finns behov av att på ett allmänt plan se över myndighetens roll och uppdrag. En brist som Datainspektionen

[11] Datainspektionens skrivelse till regeringen den 9 december 2011, dnr 1760-2011.

särskilt uppmärksammade var begränsningen i möjligheten att förena sina förelägganden och förbud med vite, särskilt i samband med tillsyn inom hälso- och sjukvården.

Utredningen om rätt information i vård och omsorg föreslog i sitt betänkande[12] att det i de föreslagna lagarna hälso- och sjukvårdsdatalagen och socialtjänstdatalagen skulle införas möjligheter för Datainspektionen att förena förelägganden eller förbud med vite.

Post- och telestyrelsens tillsyn

Post- och Telestyrelsen har dels tillsyn över de till myndigheten anmälda operatörerna, dels ett omfattande tillsynsområde vad gäller bestämmelsen om kakor som omfattar alla aktörer, inte endast anmälda aktörer på marknaden.

Post- och telestyrelsen kan genom anmälningar eller på annat sätt få indikationer om att en bestämmelse i lagen om elektronisk kommunikation inte följs, varvid myndigheten kan inleda ett tillsynsärende mot den som misstänks bryta mot lagen. Myndigheten har inte något uttalat uppdrag att hantera allmänhetens klagomål och agerar inte i enskilda konsumenters eller användares ärenden. De klagomål som kommer in till myndigheten utgör dock en viktig informationskälla och kan ligga till grund för bl.a. tillsyn och informationsinsatser.

Post- och telestyrelsen genomför också planlagda tillsynsaktiviteter för att t.ex. utreda om och hur regler följs generellt inom branschen, av en viss kategori aktörer eller avseende en viss typ av tjänst. Sådan tillsyn kan utövas, utan att det för den sakens skull finns några specifika misstankar om brister.

Enligt bestämmelser i lagen om elektronisk kommunikation, kompletterade av en direkt tillämplig EU-förordning[13] är tjänstetillhandahållare även skyldiga att rapportera inträffade integritetsincidenter till Post- och telestyrelsen och till berörda abonnenter eller enskilda personer samt att föra en förteckning över inträffade incidenter. Rapporterna ger myndigheten underlag avseende de viktigare orsakerna till integritetsincidenter, och hur tillhandahållarna arbetar

[12] Utredningens om rätt information i vård och omsorg betänkande *Rätt information på rätt plats i rätt tid*, SOU 2014:23.

[13] Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

för att förebygga och hantera inträffade händelser. Rapporterna kan även ge myndigheten anledning att misstänka att bestämmelserna om integritetsskydd inte följs och i sådana fall besluta att bedriva tillsyn.

De verktyg som Post- och telestyrelsen har till sitt förfogande är framåtsyftande. Den nuvarande regleringen ger myndigheten en möjlighet att granska operatörernas verksamhet och vid konstaterade brister förelägga om åtgärder att de vidta ta åtgärder som krävs för att förbättra säkerheten. En brist i dagens regelverk är således avsaknaden av möjligheter för myndigheten att besluta om s.k. retroaktiva sanktioner. Denna brist kan ge operatörerna ekonomiska incitament att avvakta med sådana säkerhetsåtgärder som inte kan motiveras av rent kommersiella skäl, till dess att myndigheten har meddelat eller hotar att meddela föreläggande om att vidta nödvändiga åtgärder. Incitamenten för operatörerna att självmant och på förhand vidta långtgående eller kostsamma säkerhetsåtgärder är därför små. När sårbarheter och andra brister i säkerheten uppmärksammas av Post- och telestyrelsen eller kommer till allmänhetens kännedom, så vidtar den berörda operatören oftast nödvändiga åtgärder för att komma till rätta med bristerna. Det gör att det ytterst sällan finns anledning för myndigheten att vidta några mer ingripande åtgärder, som exempelvis förelägganden, i dessa fall. Många gånger återstår det för myndigheten endast att i ett avskrivningsbeslut konstatera att brister har förelegat hos operatören, men att dessa har åtgärdats. Regleringen kan därför framstå som tandlös.

Konsumentverkets tillsyn

Konsumentverket omnämner i sin omvärldsrapport för år 2014 digitaliseringens påverkan på konsumenternas ställning, men har därutöver inte varit aktivt när det gäller integritetsskyddsfrågor, t.ex. beträffande frågor om de sociala mediernas avtalsvillkor om personuppgifter.[14]

[14] Konsumentverkets rapport 2014:13, *Vår omvärld 2014 – rapport till regeringen 2014-11-30.*

Konsumentverket har uppgivit till kommittén att det finns vissa svårigheter med tillsynen av förhållanden på internet. Problemen rör bl.a. digital och individanpassad marknadsföring på exempelvis sociala medier, baserad på en mer eller mindre ingående profilering. Företeelsen har inte varit föremål för Konsumentverkets tillsyn.

Ett splittrat tillsynsansvar

Ansvaret för tillsyn på integritetsområdet ligger alltså i dag på flera olika myndigheter. Det har i olika sammanhang diskuterats om en myndighet bör ges ett bredare uppdrag inom detta område. Exempelvis förordade Integritetsskyddskommittén[15] en utveckling och breddning av Datainspektionens roll.

Ett splittrat tillsynsansvar kan försvåra en effektiv statlig tillsyn. Dels kan det uppstå gränsdragningsproblem mellan myndigheterna. Vissa frågor eller områden riskerar då att bli förbisedda. Dels kan det leda till oklarhet för den enskilde, om vart han eller hon ska vända sig med klagomål.

Utredningen om tillsynen över den personliga integriteten, arbetar för närvarande med sitt uppdrag att lämna förslag avseende tillsynens framtida organisering.[16]

23.3 Ekonomisk ersättning

23.3.1 På vilket sätt kan ekonomisk ersättning vara ett skydd?

Den skadelidandes behov av skydd ligger till grund för utformningen av vår skadeståndslagstiftning. Lagstiftningen bygger också på antagandet om att en skyldighet att betala skadestånd kan verka preventivt mot uppkomsten att skador.[17] I förarbeten till skadeståndslagen tonades dock den preventiva funktionen ner. Det anfördes att skadeståndsreglernas moralbildande och preventiva funktion var överdri-

[15] Integritetsskyddskommitténs betänkande *Skyddet för den personliga integriteten*, SOU 2007:22, del 1, s. 489 f.
[16] Ju 2015:02.
[17] Skadeståndslagen. En kommentar m.m., femte upplagan, Bertil Bengtsson och Erland Strömbäck.

ven.[18] Diskussionen om skadeståndsrättens effekter fördes även i förarbetena[19] till de skärpta reglerna om skadeståndsansvar för föräldrar:

> När det gäller skadeståndets handlingsdirigerande – eller preventiva – effekter har debatten böljat fram och tillbaka under mycket lång tid. Vissa bedömare har menat att prevention är skadeståndets huvudsakliga funktion medan andra har menat att skadeståndsrättens viktigaste uppgift snarare är att kompensera den skadelidande. En tämligen okontroversiell slutsats som kan dras av diskussionen är att skadeståndsrätten kan ha handlingsdirigerande funktioner men att graden av handlingsdirektion varierar beroende på vilken typ av handlande som ska påverkas (vårdslöst eller uppsåtligt), andra påföljder av handlandet, försäkringsförhållanden etc.

Förarbeten till skadeståndslagen utgår alltså från att risken för att straffas för ett handlande för det mesta styr vårt handlande mer än risken för att bli ersättningsskyldig.

Det är dock inte alltid som rättsväsendet griper in när det gäller lidande som uppstår på grund av intrång mot någons personliga integritet.[20] Vissa brott som kan vara aktuella i dessa sammanhang ligger inte under allmänt åtal. När det gäller en enskild persons förutsättningar att stå upp mot företag, organisationer och myndigheter, är kanske inte anmälan till åtal det som ligger närmast till hands.

När det gäller hot och kränkningar på nätet anförs i *Näthat*[21] att det i praktiken är det bästa alternativet för den enskilde att utkräva skadestånd mot förövaren. Det framförs i boken att det är skadeståndsrätten som ger den enskilde ett rättsligt instrument för utkrävande av upprättelse när rättsväsendet kapitulerat.

Kunskapen om hur det skadeståndsrättsliga ersättningssystemet fungerar och om de faktiska effekterna är dock bristfällig.[22]

Det kan också diskuteras på vilket sätt en ekonomisk ersättning kan vara kompensatorisk för någon som drabbas av ideell skada som t.ex. en kränkning av den personliga integriteten.

---

[18] KungI. Maj:ts proposition med förslag till skadeståndslag m.m, prop. 1972:5 s, 80 ff.

[19] Regeringens proposition *Ett skärpt skadeståndsansvar för vårdnadshavare.* prop. 2009/10:142 s. 23.

[20] Näthat, Rättigheter & Möjligheter, 2:a upplagan, A. Sackemark, M. Schultz, s. 105 ff.

[21] Som ovan.

[22] *Kränkning och upprättelse, En rättssociologisk studie av kränkningsersättning till brottsoffer,* Karl Dahlstrand *(2012), s. 24 ff.*

> Det finns en inneboende slitning i synen på skadeståndets syfte vid ideell skada. Å ena sidan är det en allmän uppfattning att skadeståndet inte kan fungera som ersättning för skadan i normal bemärkelse eftersom skador av detta slag inte låter sig ersättas genom pengar. Å andra sidan så antas skadeståndet kunna ”lindra verkningarna” av skadan och kompensera känslor. Inställningen är alltså schizofren. Det ideella skadeståndet syftar till att reparera skadan, samtidigt som det råder konsensus om att skadeståndet aldrig kan reparera skadan.[23]

I en rättssociologisk avhandling[24] gjordes två enkätundersökningar för att undersöka inställningen till kränkningsersättning bland drabbade av kränkningar genom brott, och andra, som inte drabbats. Majoriteten (61 procent) av brottsoffren angav att deras ersättning antingen var av begränsad eller ingen betydelse alls för hur de mådde vid svarstillfället. För att undersöka brottsoffrens erfarenheter i relation till kränkningsersättningens funktion fick respondenterna besvara en rad frågor om vad ersättningen haft för effekter. Den funktion som ersättningen hade kunde enligt brottsoffren rangordnas från den största betydelsen till den lägsta enligt följande.

1. Ge erkännande som brottsoffer,
2. upprättelse,
3. kompensation för kränkningen,
4. kompensation för förnedringen,
5. lindra lidandet, och
6. förbättra eller återställa självkänslan.

De kommentarer, som brottsoffren lämnade i enkäten, visade att det fanns ett stort behov av att förstå vad som motiverade kränkningsersättningen. Båda enkätundersökningarna visade också att respondenterna var kritiska till rättsväsendets möjlighet att tillvarata brottsoffrens behov och intressen.

[23] Kränkning. En studie i skadeståndsrättslig argumentation, Mårten Schultz, s. 75.
[24] *Kränkning och upprättelse, En rättssociologisk studie av kränkningsersättning till brottsoffer.*

23.3.2 Möjligheten för den enskilde att begära ersättning

Generellt

En enskild person som utsatts för otillbörligt intrång i den personliga integriteten kan begära ersättning i form av skadestånd genom att väcka talan i domstol. Ersättning kan yrkas med stöd av skadeståndslagen, personuppgiftslagen och i vissa fall utan lagstöd.[25] Av lagen om elektronisk kommunikation framgår att bestämmelserna i personuppgiftslagen om bland annat skadestånd gäller även vid behandling av personuppgifter enligt denna lag.

Det finns även andra grunder för ersättning, t.ex. yrkande om ersättning med stöd av skollagen. En skolhuvudman kan få betala skadestånd till ett barn eller en elev som utsatts för t.ex. mobbning.

Sedan den 1 juli 2014 är ansökningsavgiften i allmän domstol 900 kronor i ett mål där värdet av vad som yrkas inte uppgår till mer än ett halvt prisbasbelopp och annars 2 800 kronor.

Mål om små värden

En förutsättning för att enskilda ska ha möjlighet att väcka talan om ersättning för kränkning är att det finns en faktisk möjlighet att ta hjälp av rättssystemet. Det är också en rättighet enligt Europakonventionen[26] att var och en vid prövningen av hans civila rättigheter och skyldigheter ska vara berättigad till en rättvis och offentlig förhandling inom skälig tid och inför en oavhängig och opartisk domstol, som upprättats enligt lag.

Den som yrkar skadestånd i domstol riskerar dock att vid förlust få betala motpartens rättegångskostnader. Dessa kostnader kan vara långt högre än den ersättning som yrkats.

I 1 kap. 3 d § rättegångsbalken finns därför regler om handläggning i domstol av tvister som rör ett förhållandevis lågt värde. Tanken är att tvisten ska kunna prövas av domstol utan att rättegångs-

[25] Skadestånd har utan stöd i skadeståndslagen utgått för kränkningar av grundläggande rättigheter som kommer till uttryck i Europakonventionen, NJA 2005 s. 262, statens ansvar och NJA 2009 s. 104, kommuners ansvar; jfr dock NJA 2007 s. 747, privaträttsliga rättssubjekt har inte något skadeståndsansvar under Europakonventionens regelverk. Skadestånd har också utgått för kränkningar av rättigheter uttryckta i regeringsformen, se NJA 2014 s. 323 och NJA 2014 s. 332.

[26] Artikel 6 Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

kostnaderna riskerar att bli alltför höga. Reglerna är tillämpbara för yrkanden om ersättning som är lägre än ett halvt prisbasbelopp. Förfarandet ska vara smidigt och informellt. Parterna ska normalt kunna klara av processföringen utan hjälp av juridiskt skolade ombud och ansvaret för rättegångskostnader ska vara möjligt att överblicka redan på förhand. Den som vinner tvisten kan bara få ersättning för vissa rättegångskostnader. Domstolens processledning förutsätts vara aktiv.[27]

Risken med att väcka talan om skadestånd

Om det inte är möjligt att väcka talan enligt reglerna om mål om mindre värden i 1 kap. 3 d § rättegångsbalken kan det innebära en stor risk för en enskild person att väcka talan om skadestånd. Detta kan illustreras av följande exempel. I ett mål[28] hade käranden yrkat ersättning från ett landsting på ett flertal punkter. Några av dessa avsåg ersättning för skada och kränkning på grund av brott mot personuppgiftslagen. Hennes yrkande i dessa delar bifölls i vissa delar. Tingsrättens beslut blev att landstinget skulle betala 6 000 kronor i skadestånd för dessa kränkningar och ytterligare 5 000 kronor för annan skada. Enligt tingsrätten innebar avgörandet att kvinnan endast i mindre delar hade vunnit framgång i målet och till största delen endast när landstinget medgett hennes talan. Det hon vunnit ansågs vara av ringa betydelse och hon skulle därför ersätta landstinget för dess rättegångskostnader. Tingsrätten beslutade att hon skulle betala landstingets rättegångskostnader om 1 376 832 kronor.

Statens frivilliga skadereglering

En enskild som anser att han eller hon har orsakats skada av det allmänna kan ansöka hos allmän domstol om stämning mot staten eller en kommun. Saken blir då prövad i den ordning som gäller för tvistemål.

[27] Se *Österman, Rättegångsbalk (1942:740) 1 kap. 3 d §, Lexino 2014-06-02.*
[28] Umeå tingsrätts dom den 19 juni 2014, mål nr T 1881-08.

I de fall det är fråga om en skada som orsakats av staten kan Justitiekanslern dock besluta om skadestånd till enskilda inom ramen för statens frivilliga skadereglering. Sådana anspråk från enskilda handläggs enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten. Det kan handla om anspråk som bl.a. grundas på 3 kap. 1–2 §§ skadeståndslagen eller 48 § personuppgiftslagen. Denna skadereglering är kostnadsfri för den enskilde. Han eller hon kan även få viss ersättning för ombudskostnader. Om man inte är nöjd med Justitiekanslerns beslut kan man föra talan på sedvanligt sätt inför domstol.

Några motsvarande bestämmelser som rör frivillig skadereglering på det kommunala området finns inte. Men det står en kommun fritt att själv reglera en skada som en enskild orsakats inom ramen för kommunens verksamhet, exempelvis i samband med en otillåten behandling av personuppgifter. Sådan frivillig skadeståndsreglering har enligt vad Informationshanteringsutredningen[29] uppger förekommit i endast ett fåtal fall i ett landsting eller en kommun. Om ett landsting eller en kommun inte själv vill reglera en skada, får den enskilde alltså vända sig till allmän domstol.

23.3.3 Ersättningsbeloppen vid rätt till skadestånd med stöd av personuppgiftslagen

Högsta domstolen har slagit fast[30] att kränkningsersättning enligt personuppgiftslagen ska bestämmas utifrån en bedömning av den kränkning som typiskt sett kan anses ha uppkommit. I rättsfallet sägs att ersättningsnivån i fall som inte kan anses allvarliga bör ligga under 5 000 kronor, och att ersättning för kränkningar som är att bedöma som mindre allvarliga, om än inte obetydliga, normalt bör bestämmas till ett schablonbelopp på 3 000 kronor. Av detta kan man dra slutsatsen att någon ekonomisk ersättning inte blir aktuell när en kränkning framstår som obetydlig.

I ett beslut[31] prövade Justitiekanslern skadeståndsanspråk med anledning av att personuppgifter i det s.k. Kringresanderegistret hade behandlats i strid med polisdatalagen (2010:361). Mot bak-

[29] Informationshanteringsutredningens betänkande *Myndighetsdatalag*, SOU 2015:39 s. 642.
[30] NJA 2013 s. 1046.
[31] JK:s beslut den 7 maj 2014 (dnr 1441-14-47).

grund av att det var fråga om integritetskänsliga personuppgifter och att de generella bristerna i behandlingen av dem sammantaget var allvarliga måste enligt Justitiekanslern de personer vilkas uppgifter behandlats i registret anses ha blivit utsatta för en sådan kränkning av den personliga integriteten att de var berättigade till ersättning av staten enligt 48 § personuppgiftslagen. Kränkningen kunde med hänsyn till registrets inriktning och syfte samt de brister som konstaterats inte anses som mindre allvarlig. De brister som förekommit i registret hade dock inte lett till några negativa beslut eller åtgärder som inte uppkommit om personuppgifterna behandlats helt i enlighet med polisdatalagens bestämmelser. Den som varit föremål för registrering i Kringresanderegistret borde därför vara berättigad till ersättning för kränkning med 5 000 kronor. Vid bedömningen av ersättningsbeloppets storlek beaktade Justitiekanslern vad Högsta domstolen slagit fast om att en schabloniserad bedömning i stor utsträckning kan användas.[32]

Polisens brister vid behandlingen av personuppgifter i det s.k. Kringresanderegistret kan totalt komma att kosta Polismyndigheten omkring 20 miljoner kronor till följd av krav på ersättning från de registrerade.

Från Justitiekanslerns praxis kan också nämnas två beslut där det bedömts att väsentligt högre ersättningsbelopp än vad som normalt är fallet skulle utgå. Det ena beslutet[33] rörde en person för vilken det felaktigt hade registrerats i belastningsregistret att han var dömd av norsk domstol för försök till ett grovt brott. Justitiekanslern konstaterade att det tagit exceptionellt lång tid från det att uppgifterna rätteligen borde ha tagits bort ut registret till dess att det gjordes, att det var fråga om uppgifter av mycket känslig art som var direkt felaktiga, att registreringen utgjorde ett obefogat ingrepp i personens privat- och familjeliv och att registreringen hade medfört att han tillfälligt förlorat sitt arbete. Vid en samlad bedömning bestämdes kränkningsersättningen till 25 000 kronor.

Det andra beslutet[34] rörde en person som felaktigt hade registrerats som avliden hos Försäkringskassan och Pensionsmyndigheten. Enligt Justitiekanslern hade den felaktiga registreringen rört ett mycket integritetskänsligt område. Felet hade vidarebefordrats till

[32] NJA 2013 s. 1046.
[33] JK:s beslut den 29 mars 2010 (dnr 8043-08-42).
[34] JK:s beslut den 14 oktober 2010 (dnr 1813-10-42).

premiepensionsregistret vilket hade förorsakat ytterligare problem och olägenheter. Justitiekanslern ansåg att personen i fråga hade orsakats ett betydande lidande. Han hade också under lång tid varit felaktigt registrerad som avliden. Skälig ersättning i detta fall uppgick till 30 000 kronor.

23.3.4 Fungerar ersättningssystemet i dag?

Rapporter om verkningar av ersättningssystemet

Brottsoffermyndigheten och Riksrevisionen har publicerat var sin rapport som kan vara av intresse för att belysa hur ersättningssystemet fungerar.

Brottsoffermyndigheten gav år 2014 ut en referatsamling[35] för att belysa skadeståndsrättslig praxis om kränkningsersättning vid olika typer av brott av skiftande svårighetsgrad. Brottsoffermyndigheten redovisar sju ärenden avseende ersättning vid olika typer av integritetskränkningar genom behandling av personuppgifter (beskrivna som databrott i rapporten). Av dessa utbetalades ersättning i fyra fall. Samtliga dessa avsåg ersättning vid intrång i elektroniska journaler av personal som inte hade anledning att läsa dessa journaler. Ersättningen uppgick till 5 000 kronor i två av fallen och 10 000 kronor i de andra två.

Riksrevisionen granskade år 2011[36] hur de ansvariga myndigheterna hanterar ekonomisk kompensation till personer som utsatts för brott. Riksrevisionen anför i rapporten att det för en människa som blivit utsatt för ett brott är viktigt att få upprättelse. En viktig del i upprättelsen är enligt Riksrevisionen att den som blev utsatt för brottet blir ekonomiskt kompenserad för den skada och eventuella kränkning det innebär. Riksrevisionens samlade slutsats var att det finns brister i hanteringen av brottsskadestånd. Riksrevisionen anförde att regeringen och de ansvariga myndigheterna inte gjort tillräckligt för att säkerställa en effektiv hantering av brottsskadestånd. Den information och det stöd som ges till brottsutsatta är inte till-

[35] Brottsoffermyndigheten, Referatsamling 2014.
[36] *Brottsutsatt. Myndigheternas hantering av ekonomisk kompensation på grund av brott*, RiR 2011:18.

räckligt. De brister som finns riskerar leda till att skadeståndet inte får den kompenserande effekt som avsetts. Det finns också en risk för att kravet på likabehandling inte uppfylls.

Användning av sanktion i form av ersättning

Domstolsverket kan inte ta fram statistik som visar hur många mål om ersättning i form av skadestånd enligt personuppgiftslagen som prövas i svenska tingsrätter. Kommittén har genom sökning på Infotorg endast fått fram en handfull domar. Vår sökning visar att landets tingsrätter endast avgjort fem sådana mål under perioden 2012–2015. Två av dessa ogillades utan att stämning väcktes. De tre andra prövades i sak. I två av dessa ogillades käromålet. I det tredje fick käranden en liten del av sin talan bifallen.

Domstolsverket kan inte heller ta fram statistik över mål där yrkanden har prövats om ersättning för kränkning av den personliga integriteten med stöd av 2 kap. 3 § skadeståndslagen i landets tingsrätter. Det är enligt Domstolsverket mycket osannolikt att fråga om kränkningsersättning prövats som separat mål.

Ersättningsärenden prövade av Justitiekanslern

År 2014 registrerades hos Justitiekanslern[37] 42 anspråk grundade på personuppgiftslagen och 845 anspråk grundade på skadeståndslagen eller andra skadeståndsgrundande bestämmelser, utöver anspråk på ersättning vid frihetsinskränkning, ärenden gällande det så kallade kringresanderegistret och rättegångar. År 2014 avgjorde Justitiekanslern 1 194 sådana ersättningsärenden.

Under 2014 kom därtill närmare 2 900 ersättningsanspråk in från enskilda som har varit eller trott sig ha varit registrerade i kringresanderegistret. I ett principbeslut slog Justitiekanslern fast att de brister som hade förekommit innebar att alla de personer som hade varit föremål för personuppgiftsbehandling i registret hade kränkts på ett sådant sätt att de hade rätt till viss ekonomisk ersättning. Justitie-

[37] Årsredovisning för 2014.

kanslern fann att kränkningen fick anses ha varit likartad för samtliga registrerade personer och att ersättningen skulle bestämmas till 5 000 kronor per person.[38]

23.4 Straffrättsliga sanktioner

23.4.1 På vilket sätt kan straffrättsliga åtgärder vara ett skydd?

Straffrätten utgår från hypotesen av kriminalisering kan innebära ett visst skydd mot oönskade beteenden, att straffbestämmelser har en preventiv effekt. I betänkandet *Integritet och straffskydd*[39] är utgångspunkten att det straffrättsliga skyddet bör omfatta den del av den privata sfären som brukar beskrivas som privatlivet och avse personlig information och uppgifter om privatlivet, sådant som varje individ själv bör få hålla för sig själv och bestämma i vilken mån det ska komma till andras kännedom och därmed lämna den skyddande privata sfären. Utredaren anför bl.a. att det är ett grundläggande behov hos människan att känna trygghet och välbefinnande och att hon därför måste skyddas och fredas från angrepp på sin skyddade sfär – sin personliga integritet. Sverige ska också leva upp till internationella åtaganden och vår grundlag ställer krav när det gäller både skyddet för privatlivet och skyddet för yttrandefriheten.

Olika kränkningsbrott enligt brottsbalken

Enligt direktiven[40] till *Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten* är bestämmelserna i 4 kap. brottsbalken, särskilt brotten mot någons frid, såsom olaga hot och ofredande av störst intresse när det gäller det straffrättsliga skyddet för enskildas personliga integritet på nätet. Dessa bestämmelser syftar till att skydda mot kränkningar av rent personliga intressen, som inte är av ekonomiskt slag. Vidare är ärekränkningsbrotten förtal och förolämpning i 5 kap. brottsbalken av särskilt

[38] JK:s dnr 1441-14-47.
[39] SOU 2016:7.
[40] Dir. 2014:74.

intresse. Med ära avses dels den aktning eller det anseende en person har bland sina medmänniskor, dels en persons egen känsla av att vara aktad eller ansedd.

Förslagen i *betänkandet Ett modernt och starkt straffrättsligt skydd för den personliga integriteten*[41] syftar till att göra dessa bestämmelser skarpare och lättare att tillämpa.

Dataintrång

Den som olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning ska enligt 4 kap. 9 c § brottsbalken dömas för dataintrång till böter eller fängelse i högst två år.

Bestämmelsen är t.ex. tillämplig då någon använder sig av sin behörighet till åtkomst till ett elektroniskt journalsystem för att läsa uppgifter om en patient utan att detta behövs från arbetssynpunkt, t.ex. på grund av nyfikenhet.

Bestämmelsen är också tillämplig på intrång och sabotage genom av olika typer av datavirus eller trojaner.

Brott mot personuppgiftslagen

I 49 § personuppgiftslagen föreskrivs straffansvar för den som uppsåtligen eller av grov oaktsamhet lämnar osann uppgift i information till registrerad eller till tillsynsmyndigheten, behandlar känsliga personuppgifter eller uppgifter om lagöverträdelser i strid med 13–21 §§ eller 5 a § andra stycket, brister i sin anmälningsskyldighet eller överträder förbudet mot överföring av personuppgifter till tredje land. Den som befunnits skyldig till något sådant brott ska dömas till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år.

När det gäller bestämmelsen om straff anförde regeringen i förarbetena till personuppgiftslagen[42] att de huvudsakliga sanktionerna mot de personuppgiftsansvariga som inte följer den nya lagen skulle

[41] SOU 2016:7.

[42] Regeringens proposition *Personuppgiftslag*, prop. 1997/98:44 s. 108 f.

vara skadestånd och vite. Dessa sanktioner för brott mot lagen fick anses effektiva och i stort sett tillräckliga. Det fanns dock även behov av att kriminalisera vissa olagliga åtgärder.

När personuppgiftslagen infördes omfattade straffbestämmelsen även överträdelser som begicks av oaktsamhet utan att de var grova. Genom lagändringar år 2006 avkriminaliserades oaktsamhet av normalgraden. I förarbetena anfördes som skäl bl.a. att utvecklingen hade gått mot att straff inte är en nödvändig reaktion på överträdelser av personuppgiftslagen eller anslutande registerförfattningar.[43]

Även i lagen om elektronisk kommunikation finns straffbestämmelser. Av förarbetena[44] kan utläsas att straff kan följa endast i den mån behandlingen inte är straffbelagd enligt aktuella bestämmelser i brottsbalken, som till exempel brytande av post- eller telehemlighet och dataintrång.

Straffbestämmelser med fokus främst på myndighetsområdet

Personuppgiftslagens straffbestämmelse gäller också för anställda på myndigheter. För dessa personer gäller även andra straffrättsliga bestämmelser. Ett brott inom myndighetsområdet som leder till en kränkning och som kan föranleda skadeståndsansvar enligt 2 kap. 3 § skadeståndslagen är tjänstefel enligt 20 kap. 1 § brottsbalken.

När det gäller andra brott som kan ha samband med en otillåten hantering av personuppgifter kan även brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken komma i fråga. Detsamma gäller brottet dataintrång.

I sammanhanget kan också nämnas bestämmelserna om disciplinansvar i lagen (1994:260) om offentlig anställning. Enligt dessa bestämmelser kan en arbetstagare meddelas disciplinpåföljd för tjänsteförseelse i form av varning eller löneavdrag. För detta gäller dock vissa förutsättningar, bl.a. att den misstänkta gärningen inte ska anmälas till åtal eller, om gärningen prövats i straffrättslig ordning, inte har ansetts vara något brott på grund av någon annan anledning än bristande bevisning.

[43] Regeringens proposition *Översyn av personuppgiftslagen*, prop. 2005/06:173 s. 48.
[44] Regeringens proposition *Lag om elektronisk kommunikation*, prop. 2002/03:110, s. 400–401.

Genom Arbetsdomstolens praxis har bl.a. prövats frågan om disciplinansvar för en handläggare som gjort obehöriga sökningar i Försäkringskassans datasystem.[45]

23.4.2 Fungerar straffrättssystemet i dag?

År 2013 registrerades totalt 363 anmälda brott mot personuppgiftslagen, vilket kan jämföras med exempelvis 12 731 anmälda ärekränkningsbrott under samma år.[46] Motsvarande siffor för år 2014 var 359 anmälningar om brott mot personuppgiftslagen och 13 084 ärekränkningsbrott. Under år 2014 avgjordes 32 mål om ärekränkning och 4 mål om brott mot personuppgiftslagen genom domslut, strafföreläggande eller åtalsunderlåtelse.[47] Detta år anmäldes 8 200 ärenden om dataintrång[48], medan endast 108 ärenden avgjordes.

Enligt uppgift från Datainspektionen har myndigheten polisanmält brott mot personuppgiftslagen 18 gånger de senaste fem åren. Datainspektionen har under 2015, efter begäran från polis eller åklagare, bistått med yttranden i åtta ärenden där brott mot personuppgiftslagen utretts och som gällt publicering av personuppgifter på internet.

Polisanmälningar gällande olaga hot samt förtal på Facebook har enligt en artikel i Svenska dagbladet[49] legat på runt 4 000 per år de senaste åren. Av de polisanmälningar som gäller olaga hot och förtal och som innehållit ordet Facebook har enligt samma tidningsuppgifter endast 4 procent gått vidare till åklagare.

[45] AD 2005:82.

[46] Brås rapport 2015:6, Polisanmälda hot och kränkningar mot enskilda personer via internet, s. 102.

[47] Statistiken är hämtad från Brottsförebyggande rådet. År 2010 anmäldes 420 brott mot personuppgiftslagen och 11 326 ärekränkningsbrott, år 2011 anmäldes 236 brott mot personuppgiftslagen och 11 508 ärekränkningsbrott, och år 2012 anmäldes 385 brott mot personuppgiftslagen och 12 838 ärekränkningsbrott.

[48] Det preliminära antalet anmälda dataintrång år 2015 utgör 6 580.

[49] Joanna Drevinger, Hatet på Facebook når inte domstol: ”Måste bli bättre”, publicerat på www.svd.se den 4 mars 2016.

Rapporter om sanktionssystemet

Brottsförebyggande rådet (Brå) fick år 2013 i uppdrag av regeringen att genomföra en kartläggning av polisanmälda hot och kränkningar riktade mot enskilda personer via internet. I en rapport år 2015[50] redovisades resultatet. Brå beskriver ett urval av de polisanmälda brotten, med särskilt fokus på skillnader mellan könen. Brå redovisar också i vilken omfattning de aktuella brotten lett till åtal och lagföring samt analyserar de skäl som finns till att ärenden läggs ner. I rapporten beskrivs vidare vilka problem som uppstår i rättsväsendets arbete med att utreda och lagföra de aktuella brotten. Brå ger också förslag på åtgärder mot dessa problem. Brå bedömer till exempel att polis och åklagare kan bli bättre på att använda personuppgiftslagen för att kunna lagföra kränkningar via internet. Det kräver enligt Brå att kunskapen om hur lagen kan användas på detta sätt höjs bland rättsväsendets aktörer. Flera av de händelser som i Brås material rubricerats som förtal eller ofredande borde enligt Brå även ha kunnat utgöra brott mot personuppgiftslagen. Det handlar exempelvis om ärenden där flickor har blivit uthängda på nätet med identifierbara nakenbilder och påståenden om deras sexualliv eller ärenden där domar har lagts ut offentligt på nätet.

Riksrevisionen granskade it-relaterad brottslighet år 2015.[51] Riksrevisionen anför i rapporten att vissa typer av dataintrång och bedrägerier som begås via internet i stort sett inte utreds alls. Möjligheten att nå framgång i sådana ärenden är i stort sett obefintlig i dag. Riksrevisionen konstaterar att det finns brottstyper där polis och åklagare med gällande lagstiftning och arbetssätt i stort sett saknar förutsättningar att vidta utredningsåtgärder. Sammanfattningsvis anser Riksrevisionen att både polis och åklagare behöver utveckla sina metoder och sin kompetens inom området.

23.5 Kommitténs samlade bedömning

Kommittén anser att tillsynen är ett viktigt verktyg för att åstadkomma följsamhet och respekt för gällande rätt. Detta är särskilt angeläget inom områden, där förändringstakten är hög och lagstifta-

[50] *Polisanmälda hot och kränkningar mot enskilda personer via internet*, Rapport 2015:6.
[51] *It-relaterad brottslighet – polis och åklagare kan bli effektivare*, RiR 2015:21.

ren valt en metodik för lagstiftningen, som mer eller mindre förutsätter att rättsvårdande myndigheter klargör lagbestämmelserna genom att fatta rättsliga beslut i konkreta fall. Kommittén bedömer att omfattning av tillsynen inom området inte är tillräckligt stor för att säkerställa skyddet för behandlade personuppgifter på ett önskvärt sätt.

Kommittén bedömer att de olika formerna av ekonomisk kompensation som finns, inte används i sådan omfattning som vore önskvärt för att skydda och kompensera enskilda för kränkningar av den personliga integriteten. Företag, myndigheter eller enskilda personer som begår ett otillåtet intrång i andras personliga integritet, löper mycket liten risk för att behöva ersätta den skadelidande för intrånget. Vi anser också att de belopp som betalas ut ofta är låga.

Inflytandet över hur personuppgifterna hanteras har förskjutits från den enskilde till de personuppgiftsansvariga och från de personuppgiftsansvariga till tjänsteleverantörerna, som ofta kan vara globala företag. För den enskilde innebär det bl.a. att det kan vara komplicerat att ta reda på vart man ska rikta ett anspråk på kompensation för en kränkning av den personliga integriteten.

Vidare kan den splittrade tillsynen på området leda till oklarhet för den enskilde, beträffande vilken myndighet han eller hon ska vända sig till med klagomål.

Därtill avhåller sig enskilda från att driva skadeståndsärenden på grund av att den ekonomiska risken är stor. Åklagare driver sällan frågan om skadestånd, ens när de har rättsliga möjligheter att göra det. Det ingår inte heller i Datainspektionens uppdrag att bistå enskilda i mål om skadestånd vid allmän domstol.

Kommitténs bedömning är att de straffrättsliga sanktionerna inte heller används i sådan omfattning som vore önskvärt för att kompensera enskilda för kränkningar av den personliga integriteten. Den som begår ett otillåtet intrång i andras personliga integritet, löper mycket liten risk att råka ut för någon straffrättslig sanktion. Detta, i kombination med låga straffsatser och att de bakomliggande regelverken (bl.a. personuppgiftslagen och registerförfattningarna) är relativt komplicerade, minskar den enskildes möjlighet att få till stånd lagföring eller att framställa anspråk på skadestånd. Internetrelaterad brottslighet ställer krav på både specialistkompetens och tillräckliga resurser hos Polis och åklagare.

Sammantaget bedömer kommittén därför att de skadeståndsrättsliga och straffrättsliga sanktionssystemen inte har fått den kompensatoriska eller preventiva effekt som lagstiftaren eftersträvat.

DEL V

Kommitténs förslag

24 Förslag om ökad information till regering och riksdag

Kommitténs förslag: Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet, samt till att omfatta en analys av utvecklingen. Datainspektionen ska också årligen till regeringen lämna en redovisning om utvecklingen inom området.

Regeringen ska i en årlig skrivelse till riksdagen informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet.

24.1 Integritetskommitténs uppdrag

Integritetskommittén har i uppdrag att – med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av sitt kartläggnings- och analysuppdrag – följa upp Integritetskyddskommitténs slutbetänkande[1] när det gäller behovet av att inrätta ett integritetsskyddsråd. Vi ska särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet samt föreslå nödvändiga författningsändringar.

[1] Integritetskyddskommitténs slutbetänkande *Skyddet för den personliga integriteten*, SOU 2008:3.

24.2 Integritetsskyddskommitténs överväganden

Integritetsskyddskommittén framförde i sitt slutbetänkande[2] att regeringen borde överväga vissa åtgärder för att stärka integritetsskyddet. Det anfördes bl.a. att regeringen borde överväga att i en årlig skrivelse till riksdagen informera om utvecklingen och det aktuella tillståndet rörande skyddet för den personliga integriteten. Med en sådan ordning skulle riksdagen, enligt Integritetsskyddskommitténs mening, få en samlad bild av vilka förslag som lämnats och vilka åtgärder av betydelse för integritetsskyddet som genomförts eller borde genomföras. Andra fördelar som lyftes fram var att integritetsskyddsfrågorna skulle få en politisk tyngd som de dittills saknat samt att arbetet med att ta fram underlag för skrivelsen skulle ge regeringen särskild anledning att åstadkomma samordning och skapa överblick över integritetsskyddsfrågorna inom samtliga politikområden.

Integritetsskyddskommittén pekade också på avsaknaden av ett samhällsorgan som har samlad uppsikt över den flora av apparatur och metoder som kan brukas med integritetskränkande konsekvenser samt över de tekniska möjligheter som medborgarna själva har att skydda sig mot olika former av intrång i deras privatliv. Vidare framhölls att det inte heller finns något samhällsorgan som sammanhållet tillvaratar integritetsskyddsintresset. Mot denna bakgrund föreslog Integritetsskyddskommittén att Datainspektionens roll borde utvecklas så att inspektionen tidigt uppmärksammar de teknikrelaterade riskerna för kränkningar av den personliga integriteten, utan begränsning till området för elektroniska data.

Redan i sitt delbetänkande[3] pekade Integritetsskyddskommittén på en brist på systemtänkande och helhetssyn i den integritetsskyddsrättliga lagstiftningen, som leder till att regelverket blir oenhetligt och svåröverskådligt samt försämrar möjligheterna att beakta kumulativa och samverkande effekter av nya begränsningar i integritetsskyddet som genomförs i olika delar av lagstiftningen. Integritetsskyddskommittén noterade också att inget statligt organ har i uppgift att slå larm när integritetskänslig information utnyttjas för andra ändamål än vad den varit avsedd för. Därtill konstaterade

[2] SOU 2008:3.
[3] Integritetsskyddskommitténs delbetänkande *Skyddet för den personliga integriteten* SOU 2007:22.

Integritetsskyddskommittén att takten i ny integritetsbegränsande lagstiftning i många fall var högt uppdriven. Mot denna bakgrund lyfte kommittén frågan om ett nytt särskilt organ på integritetsskyddsområdet. I slutbetänkandet återkom Integritetsskyddskommittén till denna fråga och anförde att regeringen i framtiden borde överväga inrättandet av en nämnd eller ett råd med uppgift att vaka över integritetsskyddet på hela samhällsområdet, för det fall att det skulle visa sig att kommitténs olika förslag och analyser inte ledde till ett förbättrat integritetsskydd och säkrare avvägningar i lagstiftningsprocessen.

24.3 En snabb utveckling

Den utveckling av ny teknik och nya användningsområden som skett sedan Integritetsskyddskommittén presenterade sitt slutbetänkande år 2008 har varit omfattande och har haft effekter inom i stort sett alla delar av samhället. Något som haft återverkning inom många områden är spridningen av s.k. smarta enheter (uppkopplade mobiltelefoner och surfplattor). Användingen av sådana enheter har ökat mycket snabbt de senaste åren och har haft till följd att programvaror och system har utvecklats och anpassats för att kunna fungera med de smarta enheterna. Enheternas många funktioner och sensorer innebär en stor ökning av de elektroniska spår som användarna efterlämnar i vardagen. Likaså har s.k. molntjänster på kort tid kommit att bli mycket vanliga och sådana tjänster tillhandahålls i dag av ett stort antal leverantörer för flera olika slags verksamheter. Molntjänsterna innebär ofta en global spridning av uppgifterna som hanteras och en motsvarande minskning av möjligheterna till insyn och kontroll.

En annan generell utveckling är att det blivit allt enklare att på ett samlat sätt bearbeta och analysera mycket stora datamängder av olika format (s.k. big data-analyser). Det görs ofta i realtid, vilket innebär att det blir allt svårare att i förväg veta för vilka ändamål personuppgifter kommer att användas.

I arbetet med att kartlägga och analysera risker för den personliga integriteten har kommittén särskilt noterat utvecklingen inom vissa områden. För konsumenter har det kommit allt fler kostnadsfria tjänster där motprestationen består i att konsumenten lämnar sina

personuppgifter. Allt fler vardagsgöromål, som inte uppfattas som ett uppgiftslämnande, genererar elektroniska spår – ofta utan att den enskilde är medveten om det. För skolan skräddarsys tjänster i vilka allt fler detaljerade uppgifter om elevernas förehavanden och prestationer samlas in och används för nya ändamål. Likaså blir arbetstagares vardag kartlagd, såväl avsiktligen för att effektivisera och styra verksamheter, som oavsiktligen i samband med att kunders ageranden kartläggs. Dessa är bara några exempel från de många företeelser och områden som vi har uppmärksammat. Kommittén har också noterat att det – när det kommer till statens insatser – visserligen utövas tillsyn av hur personuppgifter hanteras, men att tillsynen av naturliga skäl vanligtvis avser enstaka företeelser och inte alltid leder till att tillsynsmyndigheterna förmedlar eller ens själva får en övergripande uppfattning om den kartläggning och övervakning som faktiskt pågår.

Även när det gäller regelverket har det skett en omfattande utveckling sedan år 2008. Varje år tillkommer nya författningar eller förslag till författningar med inverkan på den personliga integriteten. I Datainspektionens publikation *Integritetsåret* (årligen 2008–2012) uppmärksammades respektive års viktigaste författningsärenden ur integritetssynpunkt. För år 2008 nämner Datainspektionen exempelvis 13 nya viktiga författningar eller författningsförslag, däribland lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen), ett förslag till ny polisdatalag, och ett förordningsförslag om ett s.k. fetmaregister. För år 2012 nämns tolv nya författningar eller författningsförslag, däribland ett förslag till ändring i signalspaningslagen med nya spaningsmöjligheter för den öppna polisen, ett lagförslag om kameraövervakning i tunnelbanan och parkeringshus samt ett förordningsförslag om befolkningsbaserad forskning.

Även under de mellanliggande åren, 2009–2011, har utvecklingstakten varit hög, att döma av Datainspektionens sammanställningar för dessa år. Sammanställningarna omfattar endast de författningar som myndigheten ansett vara av störst betydelse ur integritetssynpunkt under respektive år. Varje år får Datainspektionen emellertid långt fler författningsförslag på remiss i vilka regeringen eller remitterande myndigheter bedömt att förslagen skulle kunna vara av bety-

delse för den personliga integriteten. Som exempel kan nämnas att Datainspektionen under år 2008 svarade på 97 remisser, år 2012 på 115 remisser, och år 2014 på 117 remisser.

24.4 I Norge och Tyskland

Integritetsskyddskommittén tog i sitt slutbetänkande[4] upp den i Norge rådande ordningen som en möjlig förebild.

I Norge överlämnar regeringen varje år en skrivelse till Stortinget, bestående av Datatilsynets årsrapport och regeringens egna kortfattade kommentarer och bedömningar. I årsrapporterna redogör Datatilsynet relativt utförligt för sitt arbete på vissa utvalda områden under året, vilka resultat arbetet gett och vilka framtida utmaningar som finns inom respektive område. För sin årsrapport för år 2014 valde Datatilsynet exempelvis ut områdena hälsa och välfärd, barn och utbildning, rättsväsendet samt digitaliseringen av offentlig sektor. Fokus i redovisningarna ligger på ny teknik och nya användningsområden. I sin skrivelse till Stortinget tar regeringen sedan upp några av dessa områden. Regeringen har i skrivelsen behandlat exempelvis digitaliseringen av offentlig sektor, och bl.a. yttrat att det är viktigt att dataskyddet får en plats i denna utveckling och att det ansvariga departementet ska fortsätta sin aktiva IKT-politik och bidra till ett gott integritetsskydd.

Vidare har Datatilsynet i samarbete med det norska Teknologirådet de senaste tre åren tagit fram en mer framåtblickande och trendspanande rapport som publicerats separat. Det norska Teknologirådet är ett oberoende, offentligt organ som ger råd till Stortinget och regeringen när det gäller ny teknologi, utan begränsning till it-området.

I sammanhanhet kan nämnas att det i Tyskland råder en liknande ordning. Där överlämnar den federala dataskyddsmyndigheten (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) vart annat år en motsvarande rapport, som även innehåller förslag till åtgärder, till den parlamentariska församlingen Bundestag.

[4] SOU 2008:3.

24.5 Kommitténs överväganden och förslag

24.5.1 Behovet av ett nytt organ för säkrare avvägning i lagstiftningen

När Integritetsskyddskommittén resonerade kring behovet av ett nytt integritetsskyddsorgan, föreställde sig kommittén ett organ vars huvuduppgift skulle vara att verka för en säkrare avvägning av motstående intressen i lagstiftningen.

Enligt Integritetsskyddskommittén skulle behovet av ett sådant organ vara mindre angeläget, om det visade sig att statsmakterna skulle ta fasta på kommitténs kritiska genomgång av regelverket och förslag till lagstiftning. Det i sammanhanget mest betydelsefulla förslaget från kommittén var den nya bestämmelsen i 2 kap. 6 § andra stycket regeringsformen. Bestämmelsen innebär ett förbud för lagstiftaren att vidta åtgärder som innebär betydande intrång i den personliga integriteten, såvida inte begränsningarna görs i form av lagstiftning som är underkastad det i regeringsformen särskilt föreskrivna förfarandet vid rättighetsbegränsande lagstiftning.

Integritetsskyddskommitténs bedömningar och förslag bygger alltså på tanken att man – efter en uppföljning av effekterna i lagstiftningsarbetet av nämnda bestämmelse i regeringsformen – skulle återkomma till frågan om det finns ett behov av ett nytt integritetsskyddsorgan i kommitténs mening.

I vårt uppdrag ingår att följa upp effekterna i lagstiftningsarbetet av den aktuella bestämmelsen i regeringsformen. Som framgår ovan har denna kommitté också i uppdrag att följa upp Integritetskyddskommitténs slutbetänkande när det gäller behovet av att inrätta ett nytt integritetsskyddsorgan.

Trots att arbetet med att följa upp effekterna av ändringen i regeringsformen inte är avslutat, anser Integritetskommittén att det redan nu kan konstateras att det inte bör inrättas något nytt integritetsskyddsorgan med huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen. Datainspektionen har redan i dag ett övergripande ansvar för skyddet av personuppgifter, vilket bl.a. innebär att myndigheten regelmässigt är remissinstans (både när det gäller formella remisser och delningar från departementen) och ofta finns representerad i utredningar som gäller sådana frågor. Det finns dessutom ett flertal andra myndigheter och organisationer

som också granskar förslag till ny lagstiftning ur ett integritetsskyddsperspektiv. Här kan särskilt nämnas Justitiekanslern, Riksdagens ombudsmän, Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen, Säkerhets- och integritetsskyddsnämnden samt Advokatsamfundet, vilka ägnar ansenliga resurser åt att granska och inte sällan framföra kritik mot förslag som påverkar den personliga integriteten. De bidrar därigenom till att integritetsskyddsperspektivet lyfts fram i lagstiftningsarbetet och att bristfälliga avvägningar uppmärksammas.

Mot denna bakgrund är det Integritetskommitténs bedömning att det – oavsett vilken effekt den nya bestämmelsen i regeringsformen haft på lagstiftningsarbetet – saknas behov av ett nytt integritetsskyddsorgan som, på det sätt som Integritetsskyddskommittén ansåg kunde övervägas, skulle ha till huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen.

24.5.2 Behovet av överblick och rapportering om utvecklingen

Såväl regeringen som riksdagen har behov av kunskap för att kunna följa den snabba utveckling som beskrivs här, liksom kunskap om hur övervakning och kartläggning kan gå till och faktiskt förekommer. Kunskap behövs också om hur de legala förutsättningarna löpande förändras, vilka trender som kommer att vara av betydelse i framtiden och om hur stort det sammanlagda trycket blir på den enskilda individens privata sfär. Sådan kunskap behövs för att på olika sätt kunna påverka utvecklingen i önskvärd riktning. Kunskapen är exempelvis värdefull när det gäller att bedöma dels behov av ny lagstiftning, dels effekterna av befintlig lagstiftning och andra åtgärder som innebär att enskilda registreras eller kartläggs.

Också företag och myndigheter kan ha nytta av större kunskap och överblick, för att bättre förstå den egna rollen och få en ökad medvetenhet om sina möjligheter och skyldigheter i det digitaliserade samhället och hur dessa ständigt förändras. Även enskilda personer behöver kunna bilda sig en uppfattning om vilka aktörer som samlar in deras personuppgifter och hur uppgifterna sedan används och sprids vidare. Kunskap om detta kan bidra till att enskilda blir mer medvetna om sina rättigheter och bättre kan bedöma behovet av att vidta åtgärder för att skydda sina uppgifter.

24.5.3 Rapport till regeringen

Det finns alltså ett stort behov för staten och även samhället i övrigt av en samlad överblick över utvecklingen och dess effekter.

Det finns flera statliga myndigheter som arbetar med tillsyn av integritetsskydd. Tillsynen rör dock hur uppgifter hanteras i enskilda fall hos företag, organisationer och andra myndigheter. Tillsynsverksamheterna innebär att tillsynsmyndigheterna får goda kunskaper om sina respektive ansvarsområden, men leder inte med nödvändighet till att tillsynsmyndigheterna kan skapa sig en övergripande och sammanlagd bild av hur omfattande kartläggningen och övervakningen av enskilda faktiskt är och hur den går till i praktiken. Det gäller även Datainspektionen, trots att den myndigheten i och för sig har i uppdrag att bl.a. följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik.

Det finns alltså ett behov av att säkerställa att någon myndighet följer utvecklingen på ett mer övergripande plan och sammanfattar och analyserar nya trender, tekniker och användningsområden samt även hur de legala förutsättningarna löpande förändras.

Ett lämpligt sätt för en myndighet att åstadkomma detta är att myndigheten regelbundet tar fram och offentliggör en sammanfattning och analys av den mest aktuella och betydelsefulla utvecklingen som påverkar den personliga integriteten. En sådan sammanställning och analys skulle t.ex. kunna innehålla redogörelser för ny teknik som ännu inte kommit till användning men är under utveckling, nya företeelser och tillämpningar i Sverige, intressanta händelser i andra länder, ny lagstiftning och förslag till lagstiftning, lagförslag som blivit liggande men som är önskvärda för att stärka integriteten samt även redogörelser för områden där det finns intressekonflikter mellan den operativa verksamheten och företrädare för integritetsintresset. Det vore vidare önskvärt med en analys av den sammantagna effekten som utvecklingen har eller kan få för enskildas personliga integritet och för samhällsutvecklingen i stort. Den ansvariga myndigheten bör ges möjlighet att närmare bestämma rapportens innehåll; exempelvis är det troligen mer meningsfullt att koncentrera rapporten till några områden eller företeelser som förtjänar särskild uppmärksamhet, snarare än att eftersträva att den ska behandla all verksamhet i samhället där personuppgifter hanteras. Rapporten bör tas fram årligen och lämnas till regeringen. När utvecklingen medför

risker för den personliga integriteten, kan rapporten fungera som underlag för prioriteringar och som väckarklocka, såväl i förhållande till regeringen som till andra intressenter.

24.5.4 Skrivelse till riksdagen

Utöver att regeringen tar del av rapporten, bör det även införas en ordning där regeringen överlämnar rapporten till riksdagen i form av en skrivelse som även innehåller regeringens egna kommentarer till rapporten.

En sådan ordning – att regeringen i en årlig skrivelse till riksdagen informerar om utvecklingen och det aktuella tillståndet rörande skyddet för den personliga integriteten – ansåg Integritetsskyddskommittén att regeringen borde överväga. Med en sådan ordning skulle riksdagen få en samlad bild över vilka förslag som har lämnats och vilka åtgärder av betydelse för integritetsskyddet som har genomförts eller borde genomföras. Andra fördelar som lyftes fram var att integritetsskyddsfrågorna skulle få en politisk tyngd som de dittills saknat samt att arbetet med att ta fram underlag för skrivelsen skulle ge regeringen särskild anledning att åstadkomma samordning och skapa överblick över integritetsskyddsfrågorna inom samtliga politikområden. Integritetsskyddskommitténs förslag att regeringen borde överväga en årlig skrivelse av detta slag, har inte lett till någon åtgärd.

Vi noterar i sammanhanget att riksdagens justitieutskott[5] i en närliggande fråga, gällande regeringens årliga redovisning till riksdagen om hemlig avlyssning av elektronisk kommunikation, uttryckt att det är ett viktigt intresse från demokratisk synpunkt att diskussionen om enskildas integritet i förhållande till myndigheterna alltid hålls levande, inte minst mot bakgrund av den utveckling som har lett till att det nu finns teknik som innebär betydligt större risker för integritetskränkningar än tidigare. En minskad vaksamhet när det gäller integritetsfrågor kunde enligt utskottet leda till en avtrubbning i den allmänna uppfattningen att integritetskränkningar endast undantagsvis kan godtas i ett samhälle av den typ vi har.

[5] Bet. 1981/82:JuU54.

Integritetskommittén anser att justitieutskottets uttalande är i hög grad aktuellt även i dag, också när det gäller privata företags och organisationers hantering av personuppgifter. Även en återkommande diskussion i riksdagen om den personliga integriteten är alltjämt önskvärd. Mot den bakgrunden och även av de skäl som anfördes av Integritetsskyddskommittén, anser vi att regeringen i en årlig skrivelse till riksdagen ska informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet. Regeringen bör i detta arbete utgå från den ansvariga myndighetens årliga rapport och därutöver redovisa sin egen bedömning av utvecklingen.

Vi föreslår att denna ordning realiseras genom att regeringen årligen fattar ett beslut att lämna en skrivelse av detta slag till riksdagen.

24.5.5 Uppdraget att redovisa utvecklingen

Frågan är då vilken myndighet som bör ges uppdraget att ta fram en redovisning över utvecklingen på it-området när det gäller frågor som rör personlig integritet.

En möjlighet är att det inrättas en ny fristående myndighet för uppdraget. En sådan myndighet skulle exempelvis kunna vara uppbyggd med Genteknikнämnden som förebild. Den myndigheten har bl.a. i uppgift att genom rådgivande verksamhet främja en etiskt försvarbar och säker användning av gentekniken så att människors och djurs hälsa och miljön skyddas. Myndigheten leds av en nämnd som sammanträder tio gånger per år. Nämnden består av en ordförande och en vice ordförande som är jurister med domarerfarenhet, åtta företrädare för de politiska partierna samt sju sakkunniga ledamöter. Myndigheten har ett kansli som består av en kanslichef, en handläggare och en kanslisekreterare.

En annan möjlighet är att uppdraget ges till en redan befintlig myndighet. Ytterligare möjligheter är att det för uppdraget inrättas ett självständigt råd, i form av en myndighet, som inryms i en värdmyndighet, eller att uppdraget ges till ett universitet eller annat forskningsorgan.

En ny fristående myndighet innebär kostnader både för personal som ska utföra uppdraget och för personal som sysslar med de administrativa arbetsuppgifter som krävs på en självständig myndighet, som exempelvis registratur, lönehantering och årsredovisningar. Vidare tillkommer kostnader för lokalhyra samt för telefoner, datorer, internetanslutning och liknande.

En fristående myndighet skulle få lägga en ansenlig del av sin arbetstid på att kommunicera med den centrala myndigheten på området som är Datainspektionen, för att löpande inhämta information om inspektionens arbete och erfarenheter. I praktiken skulle en fristående myndighet i mångt och mycket vara beroende av Datainspektionen för att kunna utföra sitt uppdrag på ett bra sätt.

En fristående myndighet skulle emellertid vara fri att göra sina egna bedömningar och prioriteringar, och i det hänseendet vara oberoende i förhållande till Datainspektionen och andra tillsynsmyndigheter. Vidare kräver uppdragets utförande till viss del annan kompetens än sådan som finns samlad hos någon i dag befintlig myndighet.

Ett självständigt råd i en värdmyndighet skulle medföra lägre kostnader för administration och vissa andra poster, jämfört med en ny fristående myndighet, men har i övrigt samma för- och nackdelar som en sådan myndighet.

Även ett universitet eller annat forskningsorgan skulle vara fritt att göra sina egna bedömningar och prioriteringar, och i det hänseendet vara oberoende i förhållande till Datainspektionen och andra tillsynsmyndigheter. Ett universitet eller annat forskningsorgan som upphovsman till rapporten skulle även kunna öka den vetenskapliga trovärdigheten. Å andra sidan finns det en risk för att rapporten då också skulle bli smalare och mindre praxisorienterad än om en annan myndighet gavs uppdraget. Vidare skulle valet av universitet eller forskningsorgan komma att påverka rapportens innehåll beroende på vilken forskningsinriktning det aktuella universitetet eller forskningsorganet har. Likaså kan antas att även ett universitet eller annat forskningsorgan skulle vara i hög grad beroende av stöd från Datainspektionen för att inhämta det underlag som behövs för att utföra uppdraget.

Om uppdraget i stället skulle ges till en redan befintlig myndighet, ligger det närmast till hands att välja Datainspektionen som är den centrala myndigheten när det gäller integritetsskydd.

Det föreslagna uppdraget kan utan tvekan sägas ligga i linje med vad Datainspektionen redan i dag gör. Myndigheten ska enligt sin i dag gällande instruktion följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Hos Datainspektionen finns också en stor kompetens och erfarenhet av integritetsskyddsfrågor samlad. Den kompetensen och erfarenheten skulle kunna användas till att utföra det nya uppdraget, med viss förstärkning som kommittén återkommer till nedan. Arbetet med att ta fram rapporten skulle dessutom ge Datainspektionen erfarenheter och kunskaper som kan komma till nytta i myndighetens tillsynsarbete. Datainspektionen skulle i arbetet med att ta fram rapporten också kunna dra nytta av sina redan etablerade kontakter med andra myndigheter som arbetar med omvärldsbevakning av integritetsskyddsfrågor, som exempelvis Myndigheten för samhällsskydd och beredskap och Post- och telestyrelsen. Vidare skulle de extra kostnader, som det aktuella uppdraget skulle medföra för Datainspektionen, vara betydligt mindre än de sammanlagda kostnader som uppkommer i en ny och fristående myndighet eller i ett självständigt råd under en värdmyndighet.

Vid en samlad bedömning av frågan om uppdragets placering, anser vi att det är mest lämpligt och kostnadseffektivt att ge Datainspektionen uppdraget att vara den myndighet som ska följa utvecklingen och förmedlar en övergripande bild av dess effekter. Det kan enkelt åstadkommas genom en justering i förordningen (2007:975) med instruktion för Datainspektionen.

24.5.6 Inget rådgivande organ vid Datainspektionen

Ett uppdrag att följa och beskriva utvecklingen på området ställer höga krav på Datainspektionen, särskilt med hänsyn till utvecklingens uppskruvade hastighet.

Ett sätt att ge stöd åt Datainspektionen kunde vara att till myndigheten knyta ett rådgivande organ bestående av personer med erfarenhet från relevanta områden. Ett sådant råd skulle framför allt kunna bistå myndigheten i arbetet med att följa, analysera och beskriva utvecklingen för den personliga integriteten när det gäller att ta fram den årliga rapporten som föreslås här. Rådet skulle också kunna bistå myndigheten i annat arbete, t.ex. att ge råd angående

områden där det kan behövas särskilda åtgärder i form av informationskampanjer eller i form av möten med branschföreträdare. Dessutom skulle rådet kunna tänkas bistå myndigheten i arbetet med att ta fram separata rapporter som kan behövas för att särskilt belysa och uppmärksamma situationen inom ett visst område, vilket kan göras både på myndighetens eget initiativ eller på uppdrag av regeringen. Det kan tilläggas att ett råd av detta slag skulle ha ett annat syfte än ett insynsråd, vars uppgift är tillgodose behovet av demokratisk insyn och medborgerligt inflytande i myndighetens verksamhet.

Ledamöterna i rådet kan komma från olika verksamhetsområden. De skulle också kunna förutsättas behålla sin självständighet och sitt externa perspektiv i förhållande till Datainspektionen. Ett råd kan även bidra till att rapporten ger en allsidig och objektiv belysning av aktuella frågor.

Rådet skulle kunna bestå av experter på t.ex. teknikutveckling, teknikanvändning och lagstiftningsarbete (här benämnt expertråd). Ett annat alternativ är att rådet består av medlemmar som snarare representerar olika myndigheter och organisationer (här benämnt representationsråd) vilka skulle kunna ge rapporten en ökad tyngd och trovärdighet.

Det finns dock ett antal nackdelar och risker med att inrätta ett råd vid Datainspektionen. Den kompetens som behövs för sammanställningen och analysen kommer säkerligen att variera från år till år, beroende på vilka frågor och tekniker som är aktuella för tillfället. Det är inte särskilt troligt att medlemmarna i ett råd fortlöpande skulle kunna besitta just de specialistkunskaper som behövs för att beskriva och analysera de frågor som är av störst intresse för rapporten under ett visst år. Det gäller i synnerhet för ett expertråd, men även för ett representationsråd eftersom det inte är givet att de organsationer som finns representerade i rådet har den bästa och nyaste kunskapen på alla områden som kan bli aktuella. Om rådet inte har nödvändiga expertkunskaper, kommer det inte kunna ge något betydande bidrag till myndighetens arbete med rapporten. Datainspektionen måste då vända sig till andra externa specialister eller förlita sig enbart på egen personal. Rådet skulle i värsta fall utgöra mer av en belastning än en tillgång för myndigheten, eftersom ett råd kommer att innebära kostnader för Datainspektionen i form

av både tid och utgifter. I detta sammanhang kan nämnas att norska Datatilsynet utarbetar sin rapport till Stortinget utan bistånd av något rådgivande organ.

Det är också osäkert i vad mån ett råd skulle öka rapporternas trovärdighet och status eftersom det i första hand bör vara rapporternas innehåll och kvalitet som blir avgörande för deras trovärdighet, snarare än vilka personer eller organisationer som medverkat i framtagandet. Även utan ett råd kan regeringen uppdra åt Datainspektionen att inhämta synpunkter, erfarenheter och annat stöd från omvärlden inför framtagandet av sina rapporter.

Det är vidare inte fullständigt klarlagt om ett råd knutet till Datainspektionen skulle vara förenligt med dataskyddsdirektivets krav att de nationella tillsynsmyndigheterna ska vara fullständigt oberoende när de utövar de uppgifter som åläggs dem i nationell lagstiftning (artikel 28.1). Kravet på oberoende tillsynsmyndigheter markeras ännu tydligare i den nyligen antagna dataskyddsförordningen[6] där frågan om oberoende tillägnas en egen artikel (artikel 52).

Vid en samlad bedömning av frågan om ett råd vid Datainspektionen, anser kommittén att det är tveksamt om ett sådant skulle fylla någon viktig funktion. Vi föreslår därför inte att ett sådant råd ska inrättas.

24.5.7 Kostnader

Uppdragets genomförande innebär en omfattande omvärdsbevakning. Datainspektionen ska sedan i rapportform sammanställa och analysera observationer från omvärldsbevakningen. Vidare ska innehållet i rapporten kommuniceras till aktuella intressenter.

Hos Datainspektionen kommer uppdraget därför att kräva arbetsinsatser av personal med kompetens inom omvärldsanalys, itsäkerhet, juridik, webb och kommunikation samt administration m.m.

Därtill kommer det sannolikt krävas anlitande av konsulttjänster, t.ex. inom specialområden där myndigheten saknar tillräcklig kompetens.

[6] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

Sammantaget uppskattar kommittén att uppdragets utförande skulle kräva en kvalificerad årsarbetskraft, motsvarande cirka en miljon kronor i 2015 års kostnadsläge.

25 Konsekvenser av våra förslag

25.1 Inledning

Enligt kommittéförordningen (1998:1474) ska det i ett betänkande som innehåller nya eller ändrade regler också anges konsekvenser av dessa. Förordningen föreskriver att en sådan konsekvensanalys ska genomföras om förslagen har betydelse för den kommunala självstyrelsen, för brottsligheten, för sysselsättningen och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

I detta kapitel redogörs i korthet för Integritetskommitténs bedömning vad gäller ekonomiska konsekvenser med mera.

25.2 Ekonomiska konsekvenser

Integritetskommittén föreslår i detta delbetänkande att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet, samt till att omfatta en skyldighet att analysera utvecklingen. Datainspektionen ska också årligen till regeringen lämna en redovisning om utvecklingen inom området. Vidare föreslår kommittén att regeringen i en årlig skrivelse till riksdagen ska informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet.

Kommittén har alltså lämnat förslag om ett utvecklat myndighetsuppdrag för Datainspektionen. Detta förslag har påverkan på myndighetens resursbehov och förvaltningsanslag.

Sammantaget uppskattar kommittén att uppdragets utförande skulle kräva en kvalificerad årsarbetskraft, motsvarande cirka en miljon kronor i 2015 års kostnadsläge.

Kommittén har också föreslagit att regeringen ska få ett ytterligare rapporteringskrav till riksdagen. Detta har viss påverkan även på regeringens resursbehov.

När det gäller finansiering av den nya uppgiften vore ett alternativ att omdisponera medel inom ramen för Datainspektionens anslag. Med tanke på att kommittén vid sin kartläggning fått bilden av att myndigheten har svårt redan i dag att klara av sitt omfattande uppdrag inom befintliga ramar, föreslås inte detta. Förstärkningen bör därför göras genom en omfördelning inom utgiftsområde 4, rättsväsendet. I ett längre perspektiv bör en jämförande studie av de statliga tillsynsmyndigheternas ansvarsområden och resurstilldelning genomföras. Därefter kan nödvändiga omfördelningar göras efter angelägenhetsgrad inom denna krets.

25.3 Andra konsekvenser

I övrigt bedömer kommittén att våra förslag inte har några konsekvenser när det gäller den kommunala självstyrelsen, små företags villkor, brottsligheten och det brottsförebyggande arbetet, sysselsättning och offentlig service i olika delar av landet, jämställdheten mellan kvinnor och män eller möjligheten att nå de integrationspolitiska målen.

DEL VI

Ett dygn med familjen Svenssons elektroniska spår

Elektroniska spår under ett dygn

Personanpassade priser ... 664
Missade integritetsinställningar ... 665
Risken med dåliga lösenord ... 665
Personanpassade politiska budskap ... 666
Dåligt skämt ledde till misshandel ... 667
Barnens chattrafik okrypterad och avlyssnad ... 667
Avslöjande sökhistorik ... 668
Den skvallrande boken ... 669
E-legitimation på vift ... 670
Övervakad på jobbet och osynlig kreditprövning ... 670
Prylar som skvallrar ... 671
Kompisar som taggar utan eftertanke ... 672
Sms:et som hamnar hos polisen ... 673
Krypterade filer i molnet ... 673
Nummerplåtsavläsning ... 674
Hantering av uppgifter om hälsa ... 675
Allting spåras på webben ... 677
Utlagd i direktsändning ... 678
Elevhälsa på drift ... 679
Lifeloggingkameran som fotograferar för mycket ... 680
Kameran som vet vem den ser ... 680
Personliga länkar visar vem besökaren är ... 681
Lojalitetsapp med specialerbjudande ... 682
Ansiktsigenkänning ger bättre service ... 682
Mobiltelefonen som spårsändare i stadsplaneringen ... 683
Mobilen loggar allt och lite till … ... 684
Försäkringspremie baserad på hur familjen kör … ... 684
… och hur de lever ... 685
I skattespindelns nät ... 686
Skola i framkant ... 687
Försäkringskassan profilerar ... 688
Banken ställer frågor om penningtvätt ... 688
Kameraövervakning i sovrummet ... 689

Ett dygn med familjen Svenssons elektroniska spår

Under ett dygn lämnar familjen Svensson en stor mängd elektroniska spår efter sig av olika slag, vissa avsiktligt och andra helt omedvetet. Familjemedlemmarnas kunskap om hur uppgifterna sprids och vidareanvänds för nya ändamål varierar, liksom deras möjligheter att påverka detta. I berättelsen tar vi upp vad som i dag är tekniskt möjligt. Däremot tar vi i texten inte någon hänsyn till vad som är lagligt. Ett syfte är att få läsaren att själv reflektera över potentiellt integritetskänsliga händelser i vardagen. Många av företeelserna beskrivs närmare i andra kapitel i betänkandet.

Med den här texten vill vi visa att vanliga människor i olika vardagsituationer lämnar efter sig massor av elektroniska spår. Vi vill också ge en uppfattning om hur uppgifterna sprids och vidareanvänds. Texten innehåller exempel på teknik eller arbetssätt som redan används i Sverige eller i andra länder, samt sådant som är under utveckling och som snart kan vara verklighet.

Vi ska därför under ett drygt dygn få följa familjen Svensson, som bor i en förort till en större svensk stad. Familjen består av:

– Elisabeth, 47 år. Mamma i familjen. Arbetar som controller på läkemedelsbolag. Är rätt så teknikintresserad.

– Pär, 52 år. Pappa i familjen. Arbetar som socialsekreterare i kommunen.

– Emma, 18 år. Studerar på gymnasiet och längtar efter ett år utomlands. Jobbar ibland extra på ett callcenter i närheten.
– Vidar, 14 år. Nyfiken tonåring. Kallar sig själv tvillingbror till Ahmed.
– Ahmed, 14 år. Flydde ensam från Syrien till Sverige för två år sedan och bor nu hos familjen Svensson. Tvillingbror till Vidar.
– Tindra, 3 år. Familjens yngsta medlem. Gillar dinosaurier och är ofta förkyld.

Personanpassade priser

Det är söndag kväll. I köket står pappa Pär och lagar middag samtidigt som han pratar i telefon med sin bror. De båda familjerna planerar en gemensam solsemester. I andra änden av telefonlinjen sitter brodern och söker efter hotell och läser upp priser. Pär känner igen namnen på flera hotell, men priserna är mycket lägre än de han själv hittade kvällen innan. Han ber brodern dubbelkolla datum och – jodå, det är de två veckorna som de har tänkt resa bort.

Pär stänger av spisen, hämtar sin egen dator och sätter sig vid köksbordet och dubbelkollar priserna han hittade igår. Flera tusenlappar högre. Konstigt. Bröderna börjar om från början: Surfar till researrangörens startsida, knappar in samma datum, samma destination, samma antal personer och trycker på sök. Bröderna läser upp sökresultaten för varandra. Samma hotell, men helt olika priser. ”Vad är det här?!” utbrister Pär.

Därför blev priserna olika
Resebolaget har en personanpassad prissättning. Utifrån information om vilka bokningar en person gjort tidigare hos bolaget och de uppgifter som samlats in om personen från andra webbplatser runt om på nätet, bestäms priserna av resebolagets algoritmer. Tanken är att prisdifferentiering breddar marknaden för företag och ger dem möjlighet att nå kunder som på grund av prissättningen annars inte hade varit intresserade av deras produkter eller tjänster. Då gäller det att veta så mycket som möjligt om de potentiella kunderna. Brödernas besök och förehavanden på andra webbplatser kan kartläggas på olika sätt, exempelvis genom IP-nummer, kakor (cookies) eller samarbeten mellan olika webbplatser och annonsnätverk.[1]

[1] I kapitel 12 om konsumentområdet beskrivs närmare hur detta går till.

Missade integritetsinställningar

Samtidigt som Pär pratar med sin bror sitter Pärs fru Elisabeth vid köksbordet och skummar igenom sitt nyhetsflöde på Instabook. Plötsligt hajar hon till över Pärs senaste statusuppdatering som bara är några minuter gammal, där han spyr galla över flera av sina kollegor. Pär har redan berättat om konflikterna på jobbet för sina närmaste, men den lilla jordglobsikonen intill inlägget indikerar att bilden ligger ute helt offentligt. Hon berättar vad hon just ser för Pär, som blir alldeles kall. Så var det ju givetvis inte tänkt. Han ville bara få ur sig frustrationen och bara de redan anförtrodda skulle se det han skrev. Han inser att han gjort samma misstag som han gjort flera gånger tidigare: Han har glömt att ändra integritetsinställningarna när han skrev uppdateringen. Han raderar uppdateringen, tackar sin fru för varningen och hoppas att ingen, som inte borde, har hunnit läsa den.

Viktiga inställningar och snåriga användarvillkor
När forskare undersökte hur användare förstår integritetsinställningarna hos sociala medier, visade det sig att flertalet användare i de undersökta exemplen inte hade de integritetsinställningar som användaren hade velat ha eller trodde sig ha. I majoriteten av fallen där de faktiska inställningarna och användarnas avsikt inte stämde överrens, visades innehållet för fler än det var tänkt.

Därtill kommer att möjligheterna till att göra sekretess- eller integritetsinställningar många gånger ensidigt kan ändras av det sociala mediet. Detta är oftast helt i enlighet med användarvillkoren, som i regel är så långa och invecklade att endast få läser igenom och förstår dem.[2]

Risken med dåliga lösenord

Uppe i tonårsrummet sitter tvillingarna Vidar och Ahmed med varsin dator. När Vidar loggar in på Instabook ser han massor av inlägg postade från sitt konto. Men det är ju inte han som har skrivit dem. Han börjar skrolla och skärm efter skärm är full med länkar som leder till sidor han aldrig besökt, skrivna på ett språk han inte förstår. Vidar frågar Ahmed, men han förstår först inte alls vad som hänt.

[2] I kapitel 13 om sociala medier och e-post står det mera om integritetsinställningar och användarvillkor.

Men så kommer Ahmed på det. Förra veckan fick hackerintrånget mot webbtjänsten Snaptwit stora rubriker i media. Det stod att hela användardatabasen kommit på drift, med både användarnamn och lösenord.

”Hur kunde jag vara så dum?!”, tänker Vidar. ”Ända sedan storasyster Emma drabbades av samma sak förra året har ju mamma och pappa tjatat om att jag inte ska använda samma lösenord överallt, och att jag dessutom borde se till att aktivera tjänsten med engångslösenord som ger extra säkerhet. Kanske dags att ta tag i det där?”

Dubbel säkerhet med engångslösenord
När Vidar har aktiverat engångslösenord till de tjänster som stödjer funktionen så är det inte tillräckligt med bara hans vanliga inloggningsuppgifter för att komma in på kontot. I stället krävs en engångskod som skapas på – eller skickas till – mobilen vid varje inloggningsförsök. Funktionen kallas också tvåfaktorsautentisering. Den kan göra det mycket svårare för obehöriga att komma åt information. Ett skydd som bara består i användarnamn och lösenord kan i dag forceras på flera olika sätt. Särskilt lätt blir det när lösenordet är enkelt eller om lösenordsdatabasen har hackats och lagts ut på nätet.

Personanpassade politiska budskap

”Nu börjar det märkas att det inte är så långt kvar till valet”, säger Pär när hela familjen slagit sig ned vid middagsbordet. Han fortsätter att berätta om de politiska annonser han sett på nätet under den senaste veckan.

Elisabeth lyssnar intresserat. I slutet av Pärs uppräkning kan hon konstatera att hon bara sett två av alla de politiska budskap han exponerats för. ”Konstigt”, tänker hon.

Så fungerar personligt anpassade annonser
De politiska partierna har helt enkelt tagit till sig samma teknik som näringslivet använt i många år. Genom att på olika sätt kartlägga vilka internetanvändarna är, både i form av hårda fakta om ålder, bostadsort och kön, men också välgrundade gissningar om intressen och personliga värderingar, har de politiska partierna gått från masskommunikation till personligt anpassade budskap. Information om vilka Pär och Elisabeth faktiskt är, avgör vilka argument partierna riktar till just dem.

I USA används detta flitigt, men det är oklart i vilken utsträckning tekniken används i Sverige i dag.[3]

[3] I kapitel 12 om konsumentområdet beskrivs närmare hur detta går till.

Dåligt skämt ledde till misshandel

Under middagen berättar Ahmed att han tidigare under dagen ringde till sina kompisar i Syrien via tjänsten Ksype. Han fick då höra att en kompis råkat riktigt illa ut när han på en av landets populära mikrobloggar delat ett skämt om en ledande politikers son. Plötsligt en dag blev kompisen misshandlad på väg hem från affären och fick reda på att det skulle gå ännu värre om han inte slutade ”hålla på med omoraliska saker” på nätet. Andra kompisar vittnade om hur det var omöjligt att söka efter vissa ämnen på nätet och hur vissa inlägg på mikrobloggen ibland plötsligt var raderade. Ahmed blev också osäker – hur mycket kunde han och hans kompisar egentligen prata om detta via Ksype? ”Tänk om den tjänsten också är övervakad”, funderar han.

Myndigheterna kontrollerar nätet
Sverige har både yttrandefrihet och tryckfrihet. Men i en del andra länder har myndigheterna kontrollen över den nationella knutpunkten till internet, och använder sig av kontrollen för att övervaka och censurera all trafik som går via denna knutpunkt. Även personer som vistas i Sverige kan bli föremål för övervakning av andra länders myndigheter.[4]

Barnens chattrafik okrypterad och avlyssnad

Elisabeth oroade sig länge för hur barnen använder internet. Därför läste hon på om hur nätverk egentligen fungerar. Ganska snart hade hon skaffat den kunskap som behövs för att avlyssna trafiken i ett trådlöst nätverk, vilket hon ibland utnyttjar för att se vilka sajter barnen besöker när de stänger in sig på sina rum och använder nätet.

När Vidar går in på sitt rum efter middagen sätter sig Elisabeth vid datorn. Efter att ha betalat räkningarna tar hon ett titt på trafiken i hemnätverket och ser att Vidar just då chattar med en kurator på en organisation som stödjer barn som på olika sätt behöver hjälp. Till Elisabeths stora förvåning är chattrafiken inte krypterad och därmed väldigt lätt för henne att ta del av.

Hon brukar nöja sig med att titta på vilka webbplatser och andra tjänster barnen använder och stänger snabbt ned för att inte se vad Vidar chattar om.

[4] I avsnitt 19.4 om försvarsunderrättelseverksamhet och militär säkerhetstjänst berörs sådan övervakning.

En som däremot inte kopplar ner är grannen Veronica. För snart ett år sedan började hon läsa it-säkerhet på universitetet och passar den här kvällen på att testa sina nyvunna kunskaper. Efter att ha dömt ut säkerheten i sina föräldrars nätverk har hon gått vidare och försöker ta sig in i grannarnas nätverk.

Det blir bingo direkt! Hos Svenssons sitter någon och chattar med vad som verkar vara en psykolog eller kurator. Hon förstår snart att det är Vidar. Han är förvisso några år yngre än henne, men hon har alltid stört sig på hans alla upptåg, många gånger på gränsen till elaka eller obehagliga. Där kan man verkligen prata om någon som orsakat osämja på gatan! Det blir helt enkelt för frestande att kunna följa honom när han chattar om sina problem. Veronica följer chatten under den kvart den fortsätter, innan Vidar kopplar ner.

Inte allt är så skyddat som man kan tro …
Modern programvara som överför potentiellt integritetskänslig information via internet använder normalt, fast inte alltid, kryptering. Även när funktionen finns, kan den vara avstängd – avsiktligt eller oavsiktligt – och då kan all trafik som överförs okrypterat mellan klienten och servern lätt avlyssnas. Riskerna är störst i det lokala nätverket, särskilt om det är trådlöst.

Avslöjande sökhistorik

På kvällen skriver Ahmed det sista på inlämningsuppgiften som ska vara klar senare i veckan. Det tar några minuter innan datorn varnar för låg batterinivå. När han letat en stund efter laddaren inser han att han glömt den i skolan.

Han går in till Emma och frågar om han kan få låna hennes dator. ”Fördelen med att ha allt i molnet”, tänker han på väg tillbaka till sitt rum. Efter någon timme är han nöjd med texten. Han kollar snabbt om det hänt något kul i de sociala medierna och lämnar sedan tillbaka datorn till Emma.

Han glömmer dock att logga ut från sina konton igen. Emma blir irriterad, loggar ut honom och in i sina egna konton igen. Hon reflekterar inte över att hon därmed stänger en bakdörr in till Ahmeds hemligheter.

Skolan i molnet och datorer med spår
Skolor använder sig allt oftare av molntjänster i undervisningen. Det kan t.ex. röra sig om lärplattformar som är skräddarsydda för skolverksamhet eller om att vanliga, sociala medier används för undervisningssyften. I bägge fallen lämnar i praktiken både skolan och eleverna ifrån sig kontrollen över hur och var uppgifterna lagras och vidareanvänds.[5]

Att ha en dator där webbläsaren är inloggad till Ahmeds konton hade inte bara gett Emma möjlighet att se privata meddelanden som han skickar och tar emot. Det hade dessutom gett tillgång till hela hans sökhistorik, för lång tid tillbaka. Det kunde därmed också ha gett en detaljerad bild av vad han oroat sig för, funderat på att köpa i present till både henne själv och andra, vilka klasskamrater han varit intresserad av och så vidare.

Den skvallrande boken

Medan Pär slår på familjens smarta TV sätter Elisabeth sig i soffan med en hederlig deckare i läsplattan. Hon börjar läsa den senast inköpta boken, en del i en serie om en kvinnlig polis på Nya Zeeland. Ganska snabbt inser hon att det är samma persongalleri och upplägg som i de tidigare böckerna och klickar över till en annan bok i plattan. En halvtimme senare får hon ett mejl från e-boksförlaget som undrar varför hon sluta läsa boken och om hon skulle vilja ge något förslag till författaren. Samtidigt får Pär upp reklam på Tv:n för en bokserie om kvinnliga poliser på Nya Zeeland. Han blir något förvirrad innan han inser att han glömde att trycka på ”sin” knapp på fjärrkontrollen – den som gör att han direkt får sina personliga inställningar med mer basljud och något mer färgstark bild.

Mindre anonym mediekonsumtion
I dag uppmuntrar många medieföretag konsumenterna att logga in på sin personliga profil för att ta del av materialet. I vissa fall är detta även ett krav. På så vis går det lätt att exempelvis byta skärm och kolla färdigt på TV-serien via mobiltelefonen och det finns även andra finesser. Även utan inloggning spåras användaren så långt det är möjligt genom sammanställning av data från olika källor.

Vad som sker i bakgrunden är alltså att mediebolaget har full koll på exakt vilket innehåll som konsumenten tar del av, samt hur och när.[6] Det är kunskap som är av stort värde för både medieföretagen, deras finansiärer som exempelvis annonsörerna och även för hur sociala medier styr nyhetsflöden.

[5] I kapitel 7 om skolan beskrivs användandet av lärplattformar och sociala medier.
[6] I kapitel 12 om konsumentområdet beskrivs närmare hur detta går till.

E-legitimation på vift

Innan Elisabeth lägger sig för att sova, loggar hon med hjälp av sin e-legitimation in på Försäkringskassans webbtjänst. Hon ska justera sin inkomst efter det senaste lönelyftet, som hon var mycket nöjd med. Elisabeth har hört att det är bra att göra uppdateringen så snart som möjligt eftersom det kan påverka eventuella, framtida ersättningar. En kvart efter att hon loggat ut från kassan försöker hon med hjälp av e-legitimationen logga in på skolwebben för Vidars och Ahmeds skola. Men hon kommer inte in utan får bara ett felmeddelande. När hon nästa dag ringer banken som utfärdat e-legitimationen för att fråga om anledningen, får hon veta att e-legitimationen spärrats eftersom den strax efter utloggningen från Försäkringskassan har använts i S:t Petersburg för att logga in hos Kronofogdemyndigheten. Hon får också veta att hon enkelt kan får en ny e-legitimation utfärdad.

Blev lurad av fejkad webbsida
När Elisabeth trodde att hon loggade in på skolwebben så gjorde hon i själva verket det på en fejkad sida som liknade skolwebbens. Hackare fick då tillgång till hennes personnummer och svarskod från e-legitimationen, något som gjorde att hackarna kunde logga in hos Kronofogdemyndigheten med hennes identitet. Förhoppningsvis hann de inte orsaka någon skada innan legitimationen spärrades.[7]

Övervakad på jobbet och osynlig kreditprövning

Emma har de senaste månaderna jobbat lite extra på ett callcenter i närheten. Hennes chef är mycket nöjd med hennes arbetsinsats och har flera gånger påpekat för Emma att hon löser kundernas ärenden mycket snabbare än de flesta andra av kollegorna. Förutom att chefen i realtid kan följa hur hon löser sina arbetsuppgifter, vet chefen också exakt hur långa raster hon tar, samt vad hon säger och skriver till kunderna. Lönen är direkt kopplad till effektiviteten. Emma kan därför äntligen beställa sin efterlängtade present till sig själv – en populär smarttelefon av senaste snitt. Sent på kvällen sätter hon sig vid datorn för att beställa sin telefon.

[7] I kapitel 11 om e-förvaltning beskrivs myndigheternas kommunikation med enskilda personer i olika e-tjänster.

Men glädjen förbyts snart i besvikelse. Emma lyckas inte genomföra köpet. Hon förstår hon inte riktigt felmeddelandet hon får, men det verkar handla om att nätbutiken inte tror att hon kan betala för sig. Efter några misslyckade försök ger Emma upp. Telefonköpet får vänta.

Kreditprövning i realtid och callcenter-jobb
Emma vet inte att företaget som säljer telefoner gör en kreditprövning i bakgrunden, alltså i realtid. När hon har matat in sin e-postadress och sitt personnummer har en kreditupplysning dels genomförts på traditionellt sätt, men också genom att analysera information från öppna källor på nätet som går att knyta till henne via e-postadress och konton i sociala medier. Dessutom används en teknik som analyserar köpet i sig: tid på dygnet för köpet, typ av vara och liknande.

Verksamheter i callcenter utmärker sig som arbetsplatser genom att arbetsgivarna här ofta använder sig av sina möjligheter att kontrollera arbetstagarna i realtid på flera olika närgångna sätt.[8]

Prylar som skvallrar

Elisabeths teknikintresse har gjort att familjens hem är fullt av uppkopplade prylar: Det finns lampor, strömbrytare, rörelsedetektorer, dörrlås, termostater och flera andra saker som är anslutna till internet och som gör deras vardag lite enklare.

En av familjens favoritprylar är den wifi-uppkopplade personvågen. När en familjemedlem ställer sig på vågen skickas viktuppgifterna via familjens wifi-nät till vågtillverkarens servrar. Baserat på den senast registrerade vikten gör vågen en gissning vilken av familjemedlemmarna som nu står på vågen. Det gör att alla i familjen kan följa sina viktkurvor. Emma har även ett träningsarmband som loggar hur många steg hon tar och hur god hennes sömn är.

Familjen Svensson har också gett elbolaget rättigheter att automatiskt reglera effekten på värmepannan på nätterna mot att familjen får lägre månadsavgift – något som elbolaget flitigt utnyttjar vid tillfälliga köldknäppar. Samtidigt kan elbolaget till exempel se exakt när familjen startar sin vattenkokare på morgonen och indirekt även räkna ut om och när någon är hemma.

[8] I kapitel 8 om arbetslivet beskrivs närmare hur övervakning inom arbetslivet kan gå till.

Det är inte bara elbolaget som vet vad som händer hos Svenssons. När någon i familjen använder sin mobiltelefon för att tända lamporna i vardagsrummet går inte signalen direkt från mobiltelefon till lampa, utan den passerar först lamptillverkarens servrar: från telefonen skickas en signal till servern om vilka lampor som ska tändas, och sedan skickar servern en signal till lamporna.
Alla uppkopplade prylar innebär att många företag vet en hel del om vad som händer hemma hos familjen, dygnet runt. Mycket av informationen lagras dessutom i molntjänster.[9]

Kompisar som taggar utan eftertanke

Vidar tror inte sina ögon när han kollar telefonen efter att han vaknat. Det hjälper ju inte att han stänger av GPS-funktionen på festen i lördags kväll, om Karin ändå lägger upp bilder taggade med både adress och namn på alla personerna på bilden. ”Och så typiskt Karin att svara ja, när morsan ville följa hennes konto”, tänker han. Han skickar ett textmeddelande: ”Karin, du måste ta bort den där bilden.” Han får inget svar på textmeddelandet utan börjar i stället chatta med henne via Instabooks meddelandetjänst. Där får han kontakt. När han förklarat för Karin raderar hon bilden. ”Förhoppningsvis hann mamma inte se den”, tänker han.

Positionering och bildanalys
De i dag så vanliga smarta telefonerna innehåller, förutom kameror och sensorer, en rad olika tekniker som gör det möjligt att positionera användaren. Om alla positioneringstekniker i telefonen sätts ur bruk, blir den i praktiken obrukbar. Samtidigt utvecklar sökmotorföretagen och de sociala medierna allt mer avancerad program för att automatiskt känna igen personer på bild och film och även förstå vad som händer på dem. Förutom eventuella föräldrar och kompisar, kan bilderna och positionsuppgifterna lagras hos många olika aktörer, som t.ex. sociala medier eller apptillverkare, som i omfattande användarvillkor förbehåller sig rätten att använda uppgifterna för egna ändamål och sprida dem till olika samarbetsparter.[10]

[9] I kapitel 12 om konsumentområdet beskrivs sakernas internet och smarta elmätare.
[10] I kapitel 12 om konsumentområdet och i kapitel 13 om sociala medier och e-post behandlas appar och olika användarvillkor.

Sms:et som hamnar hos polisen

Anledningen till att Vidars textmeddelande inte kom fram var att Karins telefon nyligen stulits och att hon därför bytt telefonnummer. Hans textmeddelande hamnade i stället i händerna på polisen, som hade hittat telefonen hemma hos en misstänkt narkotikahandlare. Polisen tog mobilen i beslag och fortsatte analysera allt dess innehåll – inklusive de sms som fortfarande dyker upp i telefonen. Sms:et kan komma att ingå i förundersökningsmaterialet och utgöra allmän handling. Det kan som sådan komma att lämnas ut till den som så önskar enligt offentlighetsprincipen.

Genomsökning och kopiering av mobiltelefoner och datorer
Det är inte ovanligt att polisen bereder sig tillgång till innehållet i mobiltelefoner och datorer för att inhämta uppgifter i brottsutredande syfte. Det förekommer även att hela innehållet i mobiltelefonen eller datorn kopieras.[11]

Krypterade filer i molnet

Väckarklockan ringer tidigt nästa morgon för Elisabeth. Hon tar sig mödosamt ur sängen. ”Jag hatar de här tjänsteresorna!”, tänker hon medan hon väntar på att kaffet ska bli klart.

Efter en tågtur till grannstaden blir det taxi till kunden. Taxiresan tar 20 minuter och hon hinner slumra till i baksätet. När taxin stannar utanför kundens huvudkontor vaknar hon med ett ryck – och konstaterar att taxiresan tog mycket längre tid än den brukar. Nu är det bråttom, det här är inte en kund som har överseende med sena ankomster!

Hon slänger sig ur taxin och rusar in genom dörrarna. Det är först när hon hänger av sig kappan inne i konferensrummet som hon saknar den. Surfplattan! Hon måste ha glömt den någonstans under resan. Oturligt nog har hon avaktiverat funktionen för att kunna spåra plattan, som därmed är borta.

[11] Mer om detta finns att läsa i kapitel 18 om de brottsbekämpande myndigheternas verksamet, avsnitt 18.6.

”Katastrof! Jag har ju en massa journaler från läkemedelsstudier med enormt integritetskänsligt innehåll”, tänker hon medan hon ringer till företagets it-avdelning för att få hjälp.

Även om själva plattan är borta så visar det sig att det inte innebär någon katastrof. Efter ett beslut i ledningsgruppen så fick alla anställda nyligen en grundlig genomgång i it-säkerhet. Företagets informationssäkerhetspolicy innehåller krav på att alla bärbara prylar ska skyddas med bra lösenord och att alla känsliga dokument, som t.ex. avtalsutkast, ska lagras på företagets egna servrar i stället för lokalt i de telefoner och surfplattor som de anställda bär med sig. Alla kvarvarande uppgifter på surfplattan kan dessutom raderas på distans, något som it-avdelningen gör omedelbart efter att Elisabeth kontaktat dem.

Skadan begränsas till kostnaden för att köpa en ny platta. Elisabeth skickar en tanke av tacksamhet till företagets it-avdelning. Någon känslig information kommer sannolikt inte att hamna i orätta händer på grund av hennes slarv.

Praktiskt, men också spårbart
It-avdelningens upplägg gör att arbetsgivaren har full tillgång till hur arbetstagaren använder surfplattan, med allt vad det innebär av information om användning och positionering. Det innebär inte bara att arbetsgivaren kan följa arbetagtagarna på ett mycket närgånget sätt – utan även att den som tillverkat utrustningen eller programvaran kan lagra uppgifter som går att knyta till den enskilde arbetstagaren och dennes förehavanden.[12]

Nummerplåtsavläsning

Emma har börjat leta efter sommarjobb och blivit intresserad av ett företag som heter ParkingCheck. Vid frukostbordet berättar hon för Pär om det nystartade teknikföretaget, som sedan en tid tillbaka bedriver en intressant pilotstudie. Den omfattar bland annat parkeringsplatsen utanför mataffären där familjen brukar handla och ytterligare ett tjugotal ställen runt om i staden där det är gratis att parkera i högst två timmar.

[12] I kapitel 8 om arbetslivet beskrivs närmare hur detta kan gå till.

Tekniken är i sig lika enkel som genial. I stället för att ha parkeringsvakter som vandrar runt i staden till fots kan de nu sitta i en bil utrustad med kameror. Det är jobbet som förare av en sådan bil som Emma söker. Kamerorna filmar åt alla håll, men på mycket låg höjd för att fotografera nummerplåtar. När övervakningsbilen rullar in på en parkeringsplats startar systemet. En bild på varje registreringsskylt tas. Den behandlas med teckenigenkänning och sedan sparas registreringsnummer samt tid och plats i en databas. Sen görs en jämförelse med tidigare besök på samma plats. Är det någon av bilarna som har stått parkerad i mer än två timmar skapas automatiskt en parkeringsbot, komplett med de tidsstämplade fotografierna, som skickas hem till personen som står registrerad som bilens ägare.

Emma tycker att jobbet verkar toppen och väntar nu bara på att få besked.

Uppgifter som sparas för länge

Nummerplåtsavläsning används av en rad olika aktörer i Sverige för vitt skilda syften: alltifrån att skanna av omgivningen efter bilar med efterlysning eller körförbud, till att registrera trängselavgift.

I exemplet hade ParkingCheck (som är ett fiktivt företag) inte byggt in någon funktion i systemet som raderar data som inte längre behövs – vilket är en vanlig och generell brist hos både företag och myndigheter närt dessa hanterar uppgifter som kan knytas till enskilda personer. Om en bil som stod parkerad på ett ställe under förmiddagskollen inte finns kvar när övervakningsbilen återvänder vid lunchtid, finns det ingen anledning att behålla uppgifterna om den i systemet – men så fungerar inte ParkingChecks system. Om information som inte längre behövs sparas, innebär det att databasen med tiden kommer att innehålla en detaljerad bild av ett antal personers rörelsemönster inne i stadskärnan. Det är inte osannolikt att ett företag som ParkingCheck skulle kunna komma på något nytt användningsområde för de historiska uppgifterna.

Hantering av uppgifter om hälsa

När Pär kollar sin telefon efter morgonmötet på jobbet har han ett missat samtal från sin vårdcentral – och ett meddelande i röstbrevlådan. Det är hans läkare som ringt. ”Kan du slå mig en signal. Vi behöver diskutera resultatet efter din senaste provtagning.”

Pär har högt blodtryck och ärftlig belastning vad gäller hjärt- och kärlsjukdomar. Vid de senaste kontrollerna har blodtrycket varit för högt, så läkaren vill träffa Pär redan i dag.

Under läkarbesöket diskuterar Pär och läkaren hans livsstil och vad som kan göras för att få bättre kontroll på blodtrycket. Läkaren kommer fram till att det är bäst att börja medicinera. För att kunna göra en säker ordination vill läkaren kontrollera journaler även från andra vårdgivare. Läkaren frågar därför Pär om det är ok. Därpå klickar han sig vidare i journalsystemet och ser att det också finns uppgifter om Pär på alkoholmottagningen. Pär besökte den för ett år sedan efter att Elisabeth tjatat på honom om det. Han hade haft en period av förhöjd alkoholkonsumtion. När läkaren ser det kommer besöket att handla om hur mycket Pär dricker i dag, vilket läkaren anser vara relevant och illavarslande.

Efter besöket gör läkaren några noteringar i Svenska missbruksregistret som är ett kvalitetsregister för personer i behandling för skadligt bruk och beroende av alkohol och andra droger.

Pär å sin sida går in på landstingets webbplats och söker på ord som alkoholberoende och hamnar till sist på faktasidan om alkoholmissbruk.

Någon tid härefter händer två saker som förbryllar Pär, dels får han ett brev från en nykterhetsorganisation som ber honom som ”har egna erfarenheter av missbruk i din närhet” donera pengar till missbruksforskning, dels börjar det dyka upp reklamannonser för både avvänjningskliniker och whisky när han är ute på nätet.

Ett halvår senare beslutar en etikprövningsnämnd att uppgifterna om Pär (och om många andra registrerade) i Svenska missbruksregistret får användas i ett forskningsprojekt om alkoholens effekter för samhället. Uppgifterna kommer att samköras med en massa andra data, t.ex. om familjesituation, inkomst, vabb-dagar och vistelser inom slutenvården. Nämnden beslutar också att Pär inte behöver informeras om forskningsprojektet och inte heller behöver tillfrågas om han vill att hans uppgifter ska användas i projektet.

Den svenska forskargruppen har ett samarbete med en forskargrupp i USA. Det innebär att Pärs och de andras uppgifter lämnas ut i kodad form till gruppen i USA, i utbyte mot att den svenska gruppen får ett ekonomiskt bidrag. Inte heller detta får Pär någonsin veta och blir heller inte tillfrågad om.

Möjlighet att läsa andra vårdgivares journaler, forskning utan samtycke och patientspårning på nätet

Eftersom vårdcentralen är ansluten till ett system för sammanhållen journalföring finns Pärs journaler från andra vårdgivare som ingår i systemet tillgängliga på vårdcentralen. Detta under förutsättning att Pär inte sagt nej till detta. Den vårdgivare som vill använda de uppgifter som finns tillgängliga på detta sätt måste ha patientens samtycke till att använda uppgifterna.

Det finns omkring 100 nationella kvalitetsregister i landet som innehåller känsliga uppgifter om ett stort antal personer. Tanken med registren är att de ska göra det möjligt att utveckla kvaliteten i vården och ge underlag till forskning. Innan uppgifter hamnar i ett kvalitetsregister, ska patienten få information om registreringen och om möjligheten att stå utanför registret.[13]

Landsting kan på sina webbplatser använda sig av olika tjänster från sökmotorföretag eller sociala medier, t.ex. för att sammanställa statistik eller för att göra det lätt att dela sidan på sociala medier. Det kan innebära att landstinget i praktiken lämnar ut detaljerade och känsliga uppgifter om enskilda personers surfande till företagen bakom tjänsterna.[14]

Allting spåras på webben

Elisabeth är färdig med kundmötet och åker till företagets kontor. Hon är lite orolig för en av sina kollegor. På sistone har han inte alls verkat lika glad som han brukar och senast i förra veckan fräste han ifrån ordentligt mot två andra personer på kontoret. Dessutom har han börjat glömma sina arbetsuppgifter och kommit för sent till några möten, vilket inte alls är likt honom.

På lunchen sätter hon sig vid sin dator för att läsa om depression. Av någon anledning fick hon en ingivelse om att det är det problemen handlar om. Hon surfar runt bland några av nätets större webbplatser med sjukdomsinformation. Av en slump lägger hon märke till att en av dem har *Gilla*-knappar från Instabook. ”Undrar om det här många som gillar sidan om vattenkoppor”, tänker hon för sig själv. Däremot

[13] I kapitel 9 om hälso- och sjukvård och välfärdsteknik inom socialtjänst beskrivs kvalitetsregistren närmare. I kapitlet återges bl.a. ett verkligt ärende där patienterna fick överraskande ”tiggarbrev” som skickats ut med hjälp av uppgifter i ett kvalitetsregister. I kapitel 10 om forskning och statistik beskrivs möjligheterna att hantera uppgifter utan information eller samtycke. I kapitel 12 om konsumentområdet beskrivs hur svårt det är att anonymisera uppgifter på ett beständigt sätt.

[14] I kapitel 12 om konsumentområdet beskrivs detta närmare.

reflekterar hon inte över det faktum att knapparna över huvud taget finns på webbplatsen. Det lämnas heller ingen information på landstingets webbplats om vad Gilla-knappen innebär.

Så spåras du på nätet
Eftersom Elisabeth är inloggad på sitt Instabook-konto kan Instabook följa hennes rörelser på webben och koppla sökningarna till hennes konto, så länge sidorna hon besöker har installerat Instabook-knappar, Instabook-kommentarer eller någon av alla de Instabook-funktioner som finns. Varje gång en sida med sådana funktioner hämtas av hennes webbläsare lagras samtidigt information i Instabooks databaser om hennes surfvanor. Även utan inloggning eller eget konto, kan Instabook följa hennes rörelser på webben, fast då utan den omedelbara kopplingen till ett konto.[15]

Utlagd i direktsändning

Skolan där Vidar och Ahmed går har nyligen haft stormöte med rektorn om att vissa elever har filmat sina lärare med en ny och mycket populär direktsändningsapp under lektionerna. Ett av de inslag som diskuterades mest var sändningen med rubriken ”Vid 100 likes kastar jag min penna på läraren” som appens alla användare runtom i världen kunde se. Efter stormötet hade det blivit bättre – inga elever filmar längre sina lärare under lektionerna. Däremot har en del elever börjat filma sina klasskompisar samtidigt som de hittar på olika bus av mer eller mindre sofistikerad karaktär. I dag blev Vidar och Ahmed utsatta för knallpulver som lagts i trappan upp till kemisalarna. När de trampade på det så small det till vid varje steg som togs. ”Kanonkul”, tyckte Vidar. ”Väldigt obehagligt” tyckte Ahmed, som upplevde knallpulvret som att gå i ett minfält och tänkte på två släktingar som nyligen dött efter att ha hamnat just på ett minfält.

Appar som både sprider och samlar på sig
Förutom att det slags appar som det är frågan om i Vidars och Ahmeds skola, ibland kan användas för att kränka andra i direktsändning, samlar apparna på sig en stor mängd bildmaterial och andra uppgifter om användarna. Vissa appar ägs dessutom av företag som också äger sociala medier eller sökmotorer, vilket gör det enkelt att sambearbeta data från flera olika källor.

[15] I kapitel 13 om sociala medier och e-post beskrivs närmare hur detta går till.

Elevhälsa på drift

Under höstterminen klagade många elever i Vidars och Ahmeds skola på hög arbetsbelastning. Rektorn beslutade därför i samråd med elevhälsan att genomföra en enkät bland skolans elever och lärare. Enkäten genomförs i samarbete med en forskare på ett statligt medicinskt forskningsinstitut för att säkerställa hög kvalitet i enkätfrågorna och för att resultaten även ska komma till nytta för andra. För att göra både insamlingen och analysen så enkel som möjligt använder skolan ett webbaserat enkätverktyg. De 14-åriga eleverna instrueras av sin klasslärare att sitta i klassrummet med sina bärbara datorer och fylla i enkäten koncentrerat under vad som egentligen skulle ha varit en lektion i engelska. När alla svarat på enkäten samlar läraren in några hårstrån från varje elev, med hänvisning till att forskaren sagt att det ger ett tydligare resultat.

De ansvariga ägnade mycket tid åt att säkerställa att frågorna i enkäten skulle vara relevanta. Däremot glömde man helt bort att beakta konsekvenserna för elevernas integritet. Alla elever som under veckan följt skolledningens uppmaning och genomfört enkäten har skickat sina svar okrypterat via skolans trådlösa nätverk. Någon information lämnades inte till föräldrarna och dessa tillfrågades heller inte om deras barn skulle delta i studien.

Okrypterad överföring och forskning utan information och giltiga samtycken

Webbläsarens uppkoppling till servern där enkäten ligger var okrypterad, vilket indikerades genom att det bara stod *http* och inte *https* i webbläsarens adressfält. Den som hade lagt märke till det och förstått konsekvenserna hade kunnat avlyssna trafiken och därmed också se vilka svar skolkamraterna och lärarna lämnade.

I samarbetet mellan barnens skola och forskningsinstitutet hamnade det ”mellan stolarna” att även elevernas vårdnadshavare i förväg måste få information om hur personuppgifter kommer att hanteras inom forskningsprojektet och att det krävs ett samtycke från vårdnadshavarna. Inte heller funderade skolan över frågan om hur mycket frivillighet det egentligen kan finnas i en klassrumssituation när läraren uppmanar eleverna att delta.[16]

[16] I kapitel 10 om forskning och statistik beskrivs närmare hur detta går till. I kapitlet återges också ett verkligt ärende där man hade missat att informera och tillfråga föräldrar innan bl.a. hårstrån samlades in från eleverna.

Lifeloggingkameran som fotograferar för mycket

På väg till gymmet efter skolan berättar Emmas bästa kompis Rebecka att hon köpt en lifeloggingkamera. ”Kolla här”, säger hon och pekar på den lilla kameran som sitter fäst på hennes jacka. ”En gång var trettionde sekund tar den en bild. Hela tiden. Häftigt, eller hur?”

Emma håller med. Men i omklädningsrummet ändrar hon åsikt. Medan Rebecka går på toaletten börjar Emma byta om. Och när Rebecka kommer ut genom dörren står Emma i bara underkläderna.

”Har du fortfarande kameran på dig! Här inne?!” utbrister hon.

Rebecka ser lite förlägen ut och börjar pilla på kameran. Emma ber henne att radera bilden.

”Jag får göra det när jag kommer hem”, säger Rebecka. ”Bilderna skickas automatiskt upp till molnet och jag har inte med mig inloggningsuppgifterna. Förlåt!”.

Kameran som vet vem den ser

Callcentret där Emma arbetar har minutiös koll på hennes effektivitet, vilket också återspeglas i hennes lön. På hamburgerrestaurangen där Vidar och Ahmed jobbar extra efter skolan har alla medarbetare däremot samma lön – men alla är inte lika effektiva. Ledningen har under det senaste halvåret blivit allt mer irriterad på anställda som maskar på sina arbetspass. För att komma tillrätta med problemen har ett nytt övervakningssystem installerats. Syftet är att faktiskt mäta hur mycket tid de anställda tillbringar i personalrummet och på toaletten.

När tvillingarna använder sina RFID-taggar för att checka in när arbetspassen börjar, skickar inpasseringssystemet ett meddelande till datorerna som sköter kameraövervakningen om vem som påbörjar sitt pass.

Så fungerar kamerorna
Övervakningssystemet använder bildanalys för att hitta människor som rör sig i de områden som kamerorna täcker. Tack vare en koppling till inpasseringssystemet kan systemen tillsammans veta *vem* personen är. Kamerorna håller sedan koll på rörelser under hela arbetsdagen och sammanställer statistik över hur mycket tid medarbetarna tillbringat med arbetsuppgifter och hur mycket tid som försvunnit till annat.[17]

Personliga länkar visar vem besökaren är

Efter jobbet och besöket på vårdcentralen passerar Pär en resebyrå som i sitt skyltfönster gör reklam för specialerbjudanden på resor till Italien. ”Det kan kanske vara något för oss”, tänker han och kliver in genom dörren.

Han pratar med en av säljarna en stund och konstaterar att priserna är mycket bättre än de han och hans bror hittade när de själva surfade runt på webben igår. Han tackar för sig och säger att han kommer tillbaka senare för att göra en bokning. ”Jag måste bara prata med dem som ska med först”, förklarar han.

Säljaren erbjuder sig då att skicka en sammanställning över hotellalternativen de har tittat på. Allt hon behöver är Pärs e-postadress.

Senare på kvällen ringer han upp sin bror igen, samtidigt som han öppnar länken i mejlet som resebyrån skickade honom. Medan bröderna pratar om alternativen klickar sig Pär runt på resebyråns webbplats. Pär är inte medveten om att varje klick sparas och kopplas till honom. Trots att han inte loggat in eller på något annat sätt angett vem han är, vet resebyråns webbplats det.

Därför vet resebyrån vem han är
Länken i mejlet var personlig och kopplad till hans namn i resebyråns kunddatabas, en koppling som gjordes när han lämnade sin e-postadress till säljaren.

[17] Det står mer om möjligheterna till kameraövervakning i kapitel 20 om övervakning med kamera och i kapitel 8 om arbetslivet.

Lojalitetsapp med specialerbjudande

Nästa helg väntar två dagar i London, för att fira en god vän som nyligen fyllt 50 år. På väg hem från jobbet tar Elisabeth en sväng på stan i jakt efter en lämplig födelsedagspresent. När hon besökte inredningsbutiken där hon förra veckan varit nära att köpa en riktigt vacker vas, plingade det plötsligt till i telefonen. Med ett specialerbjudande. På just den vasen.

Elisabeth kände instinktivt att det inte kunde handla om en slump och frågade en av expediterna. Hon får veta att när hon installerade deras kundklubbs mobilapp för några månader sedan innebar det att hon godkände att de samlade in information om henne när hon besöker deras butiker.

Att ge sitt samtycke
Elisabeth minns inte, eller förstod inte riktigt att hon, när hon gick med i kundklubben och installerade appen, gav ett generellt samtycke till att detaljerad information om alla hennes förehavanden i butiken samlas in. Hon gav även samtycke till att informationen samkörs med uppgifter om henne från offentliga register och att uppgifterna kan komma att spridas till andra företag som kundklubben samarbetar med. Sammantaget kan företaget skapa en detaljerad profil av Elisabeth som kan användas för marknadsföring och produktutveckling.[18]

Ansiktsigenkänning ger bättre service

Presentjakten fortsätter. I en av butikerna har hon handlat flera gånger och hon behöver knappt kliva innanför dörrarna innan en av säljarna kommer fram och frågar om hon behöver hjälp. Men inte bara det. Han frågar också om hon är nöjd med morgonrocken som hon köpte senast. Elisabeth svarar på frågan, samtidigt som hon inte kan låta bli att imponeras av hans minne. Och förundras över hur dåligt hennes eget måste ha blivit. Hon har alltid haft svårt för att komma ihåg namn, men ett ansikte brukar hon inte glömma bort. Och den här mannen kan hon verkligen inte minnas att hon träffat tidigare. Det var förvisso några veckor sedan hon köpte morgonrocken, men hon borde ändå inte ha glömt honom.

[18] I kapitel 12 om konsumentområdet beskrivs närmare hur detta går till.

Därför kom säljaren ihåg henne
Säljaren och Elisabeth har aldrig tidigare träffats. I stället var det butikens it-system som gjorde säljaren uppmärksam på att en återkommande kund klev in över tröskeln. I butiken finns kameror som övervakar både kassorna och entrén. De sattes ursprungligen upp i säkerhetssyfte, men har kompletterats med ny mjukvara som gett dem nya funktioner: När en kund gör ett köp över ett visst belopp sparar kamerorna i kassan ett par bildrutor där kundens ansikte syns. Varje kund som passerar in i butiken matchas sedan mot alla sparade bilder. När en ”VIP-kund” kommer in i butiken görs personalen uppmärksam på det. Innan de går fram och inleder ett samtal får de på en datorskärm upp en kort sammanfattning om de senaste köpen, vilka storlekar och vilka färger och typer av plagg som kunden verkar föredra.

Mobiltelefonen som spårsändare i stadsplaneringen

På vägen hem från butikerna passerar Elisabeth en av de mest trafikerade korsningarna i staden. Det är bara en av flera platser under hennes promenad där små radiomottagare registrerar att hon – eller rättare sagt hennes telefon – passerar.

Precis som andra prylar med trådlöst nätverk letar hennes mobiltelefon ständigt efter ett wifi-nät att koppla upp sig mot. När den gör det skickar telefonen samtidigt ut sin så kallade MAC-adress, en teckensekvens som är unik för varje enhet.

Genom att samla in MAC-adresserna för de prylar som passerar på ett antal platser i stadskärnan har tjänstemännen på kommunen insett att de kan få en väldigt detaljerad bild av hur människor rör sig i stadsmiljön.

MAC-adresser inte särskilt anonyma
Visserligen finns det inga allmänt tillgängliga register som gör det möjligt att hänföra en MAC-adress till en fysisk person. Men det går ändå att identifiera en person, om uppgiften om MAC-adressen till personens mobiltelefon har sparats i ett annat sammanhang, till exempel av dennes mobiltelefonoperatör eller då personen registrerat sig i ett wifi-nätverk. Därutöver kan vanligtvis den som får tillgång till en mobiltelefon avgöra vem som är dess användare och få åtkomst till telefonens MAC-adress. MAC-adressen kan sedan användas för att knyta användaren till andra uppgifter från andra sammanhang där MAC-adressen har registrerats.[19]

[19] I kapitel 12 om konsumentområdet beskrivs olika positioneringstekniker.

Mobilen loggar allt och lite till …

”Det här var värre än jag föreställt mig”, tänker Elisabeth när hon kommer hem och tittar igenom loggfilen som hon precis har fått från sin operatör. Efter många om och men har hon fått företaget att lämna ut all information som hon har efterfrågat. Databasen innehåller information om vilka av operatörens basstationer Elisabeths telefon har kopplat upp sig mot. Därmed går det att se var mobilen – och följaktligen även hon – befunnit sig, timme för timme, dag för dag, under de senaste sex månaderna. ”Det vill verkligen till att operatören har koll på vilka som får titta på den här informationen”, tänker hon.

Datalagringskrav att spara uppgifter i ett halvår
Av loggfilen som Elisabeth fått går det bland annat att dra slutsatser om hennes pendlingsväg till och från jobbet, vilka kvarter hon brukar välja under luncherna och vilket friluftsområde hon regelbundet besöker för helgens löprunda. Operatörerna är enligt datalagringsdirektivet skyldiga att spara data i sex månader.[20]

Försäkringspremie baserad på hur familjen kör …

Elisabeth suckar när går igenom dagens post. Kuvertet från försäkringsbolaget påminner henne om att hon och Pär verkligen borde se över bilförsäkringen. Sedan hon bytte jobb för ett halvår sedan rullar bilen betydligt mer och det måste givetvis försäkringsbolaget få reda på så att de betalar rätt premie.

Hon sprättar upp kuvertet och börjar läsa. ”Det här är ju perfekt!” tänker hon. I brevet som följer med fakturan presenterar försäkringsbolaget en ny tjänst. I stället för att låta premien beräknas på en uppskattad körsträcka kan den beräknas på hur långt bilen faktiskt rullar. Allt som behövs är lite ny teknik. Försäkringsbolaget erbjuder två alternativ: Antingen en app som installeras i mobiltelefonen eller en liten dosa som monteras i bilen. Grundprincipen är dock densamma oavsett teknisk lösning. Sensorer känner av accelerationer, inbroms-

[20] I avsnitt 18.5 i kapitel 18 om brottsbekämpning skriver vi mer om tjänsteleverantörernas skyldighet att spara och i vissa fall lämna ut trafik- och lokaliseringsuppgifter.

ningar och kurvtagning medan en GPS-enhet loggar var och hur snabbt bilen färdas. Utifrån den insamlade informationen räknas ett förarbetyg ut. Högt betyg innebär rabatt på försäkringspremien.

Brevet från försäkringsbolaget tar däremot inte upp på vilka andra sätt informationen kan och får användas. Elisabeth, som regelbundet tar bilen till sin psykolog, funderar på om den informationen möjligen kan påverka premien på den sjuk- och olycksfallsförsäkring hon har hos samma bolag. Och Pär brukar ju faktiskt bryta mot hastighetsbegränsningarna både ofta och mycket. ”Betyder det både högre premie och en risk för böter i efterhand?”

I brevet medföljer avtalstexten som består av fyra sidor tätt skriven text. Elisabeth börjar läsa igenom den, men kommer inte längre än till hälften på den första sidan innan hon ger upp. Så mycket förstår hon dock att informationen kan komma att säljas vidare till försäkringsbolagets partners och delas med externa datamäklare – något som gör henne ännu mer tveksam.

… och hur de lever

När hon läst klart brevet tar hon fram sin dator och börjar surfa runt på försäkringsbolagens webbplatser för att se om det är fler bolag som erbjuder samma lösning. Hon hittar ett par stycken, och dessutom två som erbjuder prestationsbaserade premier även på personförsäkringar. Med ett aktivitetsarmband registrerar försäkringstagaren både sina träningspass och sin vardagsmotion och dessutom sin puls. Det finns en sensor som placeras under madrassen kan mäta sömnkvalitet och en fjärde pryl kan registrera stressnivåer. En uppkopplad personvåg som kan rapportera in viktutvecklingen har ju familjen redan – så där skulle steget inte vara långt. Det räcker med att ge bolaget tillgång till vågens data. Kunderna väljer själva vilka av prylarna de är intresserade av, och för vart och ett av mätvärdena finns olika rabattnivåer utifrån mätresultat.

”Min vikt är ju under kontroll och jag skulle säkert få bra värden också genom de övriga prylarna”, säger Elisabeth till Pär.

”Men det där låter inte som någonting för mig”, säger Pär. ”Jag är ju lite överviktig och stressad på jobbet vilket dessutom leder till sena kvällar, dålig nattsömn och minimalt med tid till träning. Inte

heller skulle det vara något för brorsan. Ensamstående med två barn. Det finns inte en chans att han eller jag skulle ha möjlighet att leva upp till de här kraven på massor av träning och tillräcklig sömn.”

Även om Elisabeth inser att hon personligen skulle tjäna några kronor på upplägget tvekar hon. Hon tycker inte att det känns bra att låta ett företag få veta så mycket om hennes liv. Hon förstår att alla uppgifter, åtminstone i normalläget, bara kommer att bearbetas av datorer utan att en människa tittar på dem. Men all informationen kommer ändå finnas där, hos försäkringsbolaget och kanske också i någon molntjänst utanför EU. Svart på vitt om hur hon tränar, sover, stressar.

Individualiserade försäkringar och värdefulla uppgifter

Möjligheterna att genom olika former av digitala egenmätningar lämna underlag för beräkning av försäkringspremier, t.ex. för fordonsförsäkring och personförsäkring innebär fler elektroniska spår och därmed nya integritetsrisker.[21]

Det finns också risk för att tredjepartsintressenter vill ta del av de uppgifter som samlas in. Datamäklare lever på att sammanställa personuppgifter från olika källor och i sin tur sälja dem vidare. Positioneringsdata kombinerad med körstil kan säljas till företag som vill skicka effektivare direktreklam hem till familjen Svensson.[22]

I skattespindelns nät

Bland räkningarna och reklamen finns ett brev från Skatteverket till Pär. När han öppnar det får han se att det är en handläggare som ställer frågor om hans försäljning av porslin på nätet. Han har alltid varit svag för snyggt porslin och köper på sig långt mer än vad familjen behöver, men säljer regelbundet av en del när han hittar något nytt. Till slut har det blivit något av en hobby, och han gillar också att han träffar på många trevliga människor genom sitt intresse. Men nu är det tydligen något som Skatteverket intresserar sig för. I brevet anges exempel på några nyligen genomförda försäljningar. Pär undrar

[21] I kapitel 14 om försäkringsverksamhet skriver vi mera om hantering av uppgifter i försäkringsföretagen.

[22] I kapitel 12 om konsumentverksamhet skriver vi mera om det ekonomiska värdet av personuppgifter.

vad de egentligen prioriterar på Skatteverket, om de låter folk sitta och söka av alla begagnatsajter. Lite obehagligt tycker han också att det känns, att de har sådan koll på vad han gör.

Spindlar hittar begagnat porslin
Det inte är människor som söker av nätet efter oredovisade skatteintäkter. Det jobbet görs av Skatteverkets särskilda programvara, s.k. spindlar, som automatiserat och outtröttligt söker av olika typer av webbplatser efter skattepliktig verksamhet.[23]

Skola i framkant

På kvällen dagen efter problemet med skolwebben för Elisabeth, gör i stället Pär ett försök att logga in. Han har ett oläst meddelande från skolan där det står att Vidar snart kan komma att behöva extra lektioner i engelska. Även om Vidar inte har några större problem att hänga med i dagsläget, har tydligen en s.k. ”prediktiv” analys av hans sätt att använda sig av det digitala läromedlet i engelska visat att det finns en risk för att han kommer att hamna efter inom en snar framtid.

Prediktiv analys går ut på att förutsäga framtida händelser med hjälp av stora mängder data och smarta algoritmer. I Vidars fall handlar det om att alla detaljer analyseras i minsta detalj – från hans chatt med hjälppersonerna och klick på faktarutorna i elevplattformverktyget, till vilka han umgås och interagerar med.

Prediktiv analys
Prediktiv analys i skolan är en del av det som ibland kallas för learning analytics. Här handlar det i stor utsträckning om att arbeta med uppgifter om enskilda individer, till skillnad från traditionell dataanalys, som är mer inriktad mot kluster eller grupper av individer. I dagens digitala skolwebbar, lärplattformar och läromedel, skapas en rad elektroniska spår om varje enskild elev. Det kan röra sig om alltifrån hur eleven löser uppgifter till vilka han eller hon chattar med i verktyget. I learning analytics används uppgifterna till att förbättra system och läromedel och för att få veta mer om enskilda elever. Detta finns redan i vissa länder, men det är oklart hur utbrett det är i Sverige.[24]

[23] I kapitel 11 om e-förvaltning beskrivs Skatteverkets kontrollverksamhet.
[24] I kapitel 7 om skolan beskrivs detta mer utförligt.

Försäkringskassan profilerar

Tindra börjar hosta och verkar plötsligt ha fått feber. Det är tydligt att någon kommer att behöva vara hemma med henne i morgon – och den här gången är det Elisabeths tur att vabba. Elisabeth e-postar sina kollegor och förklarar att hon kommer vara nåbar i hemmet i morgon. Tack vare den bärbara datorn kan hon koppla upp sig mot jobbnätverket och på jobbmobilen. Hon anmäler och ansöker också om tillfällig föräldrapenning på Försäkringskassans webbplats med hjälp av sin e-legitimation. ”Så smidigt” tänker hon som tidigare missat flera dagar av föräldrapenning på den tiden när hon ansökte på pappersblankett och dessutom behövde ett frånvarointyg från förskolan.

Automatiserat kontrollsystem
Vad Elisabeth inte känner till är att hennes ansökan utlöser en intern impuls till en handläggare på Försäkringskassan att kontakta förskolan för att kontrollera att Tindra verkligen inte är på plats. Anledningen är att Elisabeth av kassans automatiserade kontrollsystem kategoriserats som en person som behöver kontrolleras oftare än andra. Kassan har inte informerat Elisabeth om detta eller om vilka faktorer som avgjort att hon ska kontrolleras mer än andra.[25]

Banken ställer frågor om penningtvätt

Strax före läggdags ringer Pärs mor och låter besvärad. Det är inte ofta hon har tid att tala med Pär på telefon nu för tiden. Sedan hon i september blev invald i riksdagen har hon knappt haft en ledig stund. Det hon nu vill tala om rör hennes uppdrag som riksdagsledamot, men angår även Pär och hans familj. När hon nyligen skulle byta bank hade den tilltänkta banken fått reda på att hon blivit invald i riksdagen. Därför behövde nu banken ha ett möte med den nyblivna riksdagsledamoten, hennes man och deras barn, för att ställa frågor om hela släktens ekonomi.

Pär blir fundersam efter samtalet, eftersom han nyligen haft diskussioner med samma bank angående möjligheten att få ett lånelöfte för att kunna köpa ett sommarställe som han och Elisabeth länge drömt om. ”Kommer det här att påverka våra möjligheter att få

[25] I kapitel 11 om e-förvaltning beskrivs Försäkringskassan kontrollverksamhet.

det där lånelöftet?” undrar han. Han tänker också tillbaka på att han och Elisabeth för ett år sedan fått låna en större summa räntefritt av sin mamma för att kunna köpa ny bil.

Politically Exposed Person
En person i politiskt utsatt ställning (på engelska *Politically Exposed Person*) är en person som genom sin position och sitt inflytande anses inneha en ställning som i sig utgör en risk för att utnyttjas för bl.a. mutbrott och andra former av korruption och i förlängningen penningtvätt, liksom för aktiviteter som kan relateras till finansiering av terrorism. Tanken är att bankerna inte ska kunna utnyttjas för penningtvätt eller finansiering av terrorism.[26]

Kameraövervakning i sovrummet

Strax före midnatt på måndagskvällen ringer telefonen hemma hos familjen Svensson. Det är från seniorboendet där Elisabeths föräldrar bor sedan ett halvår tillbaka. Kameraövervakningen i deras lägenhet har larmat. Elisabeths pappa har trillat ur sängen och sedan inte lyckats resa sig på egen hand. Personalen har varit där och hjälpt honom upp och kunde efter en kort undersökning konstatera att det inte hade hänt något allvarligt den här gången. Det visade sig att han hade sovit så djupt att han inte hade vaknat när han råkade rulla ur sängen.

Efter att ha lugnat ned sig efter det sena telefonsamtalet känner sig Elisabeth nöjd med beslutet att låta installera övervakningskamerorna.[27] De skiljer sig från traditionell kameraövervakning som kräver att en människa tittar på vad som händer. Här är det i stället algoritmer som analyserar dataströmmen och kan ”se” vad människor som rör sig i det övervakade området gör. Systemet är konstruerat för att larma i sådana situationer som den som inträffade ikväll, när någon hamnar på golvet och blir liggande där utan att resa sig upp igen.

[26] I kapitel 15 om bank- och kreditmarknaden finns mer att läsa om bankernas behandling av personuppgifter för att uppfylla rapporteringskrav m.m.
[27] I kapitel 20 behandlar vi de generella frågorna om kameraövervakning. I kapitel 9 om hälso- och sjukvård och välfärdsteknik inom socialtjänst skriver vi om kameraövervakning som välfärdsteknik.

Att installera kameror i sina föräldrars hem hade inte på något sätt varit ett självklart beslut, men både hennes mamma och pappa hade insisterat. De uppskattar den trygghet som kameran ger och säger att de skulle uppleva det som oroligt och mer integritetskränkande att någon från hemtjänsten skulle komma in till dem mitt i natten.

Övervakning som välfärdstjänst
Övervakning med hjälp av robotar, videokameror och GPS-sändare kan användas som ett alternativ eller ett komplement till vård- och omsorgspersonalens fysiska tillsyn av en äldre person i hans eller hennes hem. Det kan finnas flera syften med att använda övervakning. Ett syfte kan vara att stärka den enskildes självbestämmande och integritet genom att han eller hon i större utsträckning själv kan bestämma över sin vardag. Andra syften kan vara att förbättra säkerheten för den enskilde eller att spara in på personalresurser.[28]

[28] I kapitel 9 om hälso- och sjukvård och välfärdsteknik inom socialtjänst behandlas användningen av välfärdsteknik inom socialtjänsten i avsnitt 9.6.

DEL VII

Reservation

Reservation

Reservation av ledamöterna Agneta Börjesson och Maria Ferm, miljöpartiet

Miljöpartiet har länge drivit frågan om att stärka den personliga integriteten. Något som har blivit än viktigare med den utveckling som har skett de senaste åren som inneburit att allt mer personlig information finns tillgänglig på internet och hos olika myndigheter och företag. Frågor rörande skyddet av enskildas privatliv och uppgifter kring dem, hanteras av ett antal olika myndigheter i Sverige. Datainspektionen hanterar personuppgifter generellt i samhället, Säkerhets- och integritetsskyddsnämnden har hand om känsliga personuppgifter hos Säkerhetspolisen och användandet av hemliga tvångsmedel hos polisen och Åklagarmyndigheten. Justitiekanslern har tillsyn över all offentlig verksamhet och utöver detta finns organ som Pressens opinionsnämnd och den kontroll som sker genom domstolar.

Integritetsskyddskommittén konstaterade i sitt delbetänkande 2007 (SOU 2007:22 Skyddet för den personliga integriteten) att det i Sverige finns en brist på systemtänkande och helhetssyn när det gäller integritetsskyddet, vilket leder till att regelverket blir oenhetligt och svåröverskådligt. Integritetsskyddet har en svag ställning i Sverige och inget statligt organ har i uppgift att slå larm när integritetskänslig information utnyttjas till fel ändamål. Detta har lett till en fragmentarisk bild över hur olika lagstiftningsåtgärder påverkar enskildas integritet och en avsaknad av en helhetsbild i landet. Miljöpartiets bedömning är att detta samlade skydd kan erhållas genom inrättandet av ett integritetsskyddsråd eller en integritetskyddsmyndighet med ett samlat ansvar för skyddet av enskildas integritet. Endast ett representationsråd vid Datainspektionen, anser Miljöpartiet inte är tillräckligt

för att på ett tillfredsställande sätt stärka den personliga integriteten. Vi reserverar oss därför mot att kommittén vid sitt ställningstagande till denna fråga inte lämnat något sådant förslag.

I övriga delar ställer vi oss bakom delbetänkandet.

Bilagor

Kommittédirektiv 2014:65

Den personliga integriteten

Beslut vid regeringssammanträde den 8 maj 2014

Sammanfattning

En parlamentariskt sammansatt kommitté ska

- utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet samt inom ramen för detta arbete följa upp effekterna i lagstiftningsarbetet av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes 2011, och
- med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av kartläggnings- och analysuppdraget, följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd och särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet, samt föreslå nödvändiga författningsändringar.

Kommittén får, om den bedömer att det är lämpligt, lämna ett eller flera delbetänkanden. I uppdraget ingår inte att föreslå ändringar i grundlag.

Uppdraget ska redovisas slutligt senast den 1 december 2016.

Bakgrund

Grundläggande bestämmelser om personlig integritet

Begreppet personlig integritet används i vardagligt tal vanligen för att beteckna individens värde och värdighet. Begreppet finns i både grundlag och vanlig lag, t.ex. 2 kap. 6 § andra stycket regeringsformen (RF) och 5 a § personuppgiftslagen (1998:204). Någon allmängiltig definition av begreppet har dock inte slagits fast i lagstiftningen. I ett försök att ändå beskriva vad som kan anses vara kärnan i rätten till personlig integritet har lagstiftaren uttalat att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas (prop. 2009/10:80 s. 175, prop. 2005/06:173 s. 15). I Nationalencyklopedins ordbok beskrivs den personliga integriteten som en ”rätt att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp”. Rätten till personlig integritet kan också beskrivas som en rätt att bli lämnad i fred eller en rätt till självbestämmande och valfrihet.

Grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet finns i bl.a. regeringsformen. Av målsättningsstadgandet i 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Vidare finns i 2 kap. 6 § RF en bestämmelse som slår fast ett skydd för förtroliga meddelanden och som även stadgar att var och en också i övrigt är skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten som sker utan samtycke och innebär kartläggning eller övervakning av enskilds personliga förhållanden.

Enligt artikel 8 i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), som gäller som svensk lag, har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Av 2 kap. 19 § RF följer att en lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen. En bestämmelse om respekt för privat- och familjelivet finns även i artikel 7 i Europeiska unionens stadga om

de grundläggande rättigheterna. Av artikel 8 i stadgan följer vidare bl.a. att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Rätten till skydd av privatlivet och den personliga integriteten är inte absolut. Skyddet enligt regeringsformen kan inskränkas genom lag (2 kap. 20 § RF). Begränsningarna får dock inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett dem och inte heller sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen. Det fordrar bl.a. att nya lagförslag, som innebär risker ur integritetssynpunkt, är väl motiverade och grundade på noggranna behovsanalyser och intresseavvägningar, att konsekvensbeskrivningarna när det gäller integritetsaspekterna är klara och begripliga samt att det är möjligt att förstå varför ett förslag valts framför ett annat, mindre ingripande, förslag för att nå ett visst eftersträvat mål (SOU 2007:22 s. 445 f.). Finns det utrymme att vidta särskilda åtgärder för att begränsa intrångets intensitet måste sådana normalt övervägas och om möjligt också vidtas. Intresset av enskildas personliga integritet måste således vägas mot andra berättigade intressen i samhället, t.ex. yttrandefrihet, ett tryggt och säkert rättssamhälle och en effektiv förvaltning. Även skyddet för privatlivet enligt Europakonventionen får begränsas för vissa närmare angivna ändamål men bara i den utsträckning inskränkningarna är nödvändiga i ett demokratiskt samhälle. Motsvarande begränsningar får göras enligt EU:s stadga för de grundläggande rättigheterna.

Europadomstolen har i sin praxis slagit fast att artikel 8 i Europakonventionen ålägger staten såväl en negativ förpliktelse att avstå från att göra intrång i rätten till respekt för privat- och familjelivet som en positiv förpliktelse att skydda enskilda mot att andra enskilda handlar på ett sätt som innebär integritetsintrång (se t.ex. Airey mot Irland, dom den 9 oktober 1979, § 32, Serie A nr 32 och X och Y mot Nederländerna, dom den 26 mars 1985, § 23, Serie A nr 91).

Tidigare och pågående utredningar om integritetsskydd

År 1966 fick Integritetsskyddskommittén (Ju 1967:62) i uppdrag att utreda förutsättningarna för ett stärkt skydd på personrättens område. Arbetet, som redovisades i fyra betänkanden (Skydd mot avlyssning, SOU 1970:47, Fotografering och integritet, SOU 1974:85, Reklam

och integritet, SOU 1976:48 och Privatlivets fred, SOU 1980:8), resulterade bl.a. 1975 i lagstiftning om straff för olovlig avlyssning och 1977 i lagstiftning om TV-övervakning (i nuvarande lagstiftning benämnd kameraövervakning). Frågor om skydd mot intrång i privatlivet har därefter även behandlats av bl.a. Yttrandefrihetsutredningen (Värna yttrandefriheten, SOU 1983:70), Data- och offentlighetskommittén (Integritetsskyddet i informationssamhället 3. Grundlagsfrågor, Ds Ju 1987:8), Personnummerutredningen (Personnummer – integritet och effektivitet, SOU 1994:63), Datalagskommittén (Integritet – Offentlighet – Informationsteknik, SOU 1997:39) och Utredningen om integritetsskydd i arbetslivet (Integritetsskydd i arbetslivet, SOU 2009:44). Detta utredningsarbete har bl.a. resulterat i en grundlagsändring 1989 (tidigare 2 kap. 3 § andra stycket RF) och införandet av personuppgiftslagen 1998. I maj 2013 beslutade regeringen direktiv till en särskild utredare (A 2013:04) som bl.a. ska undersöka i vilken utsträckning och av vilka skäl arbetsgivare begär att få se utdrag ur belastningsregistret från arbetssökande och i vilken utsträckning det förekommer att arbetsgivare begär att redan anställda visar upp sådana registerutdrag (dir. 2013:56). Uppdraget ska redovisas senast den 30 april 2014.

Regeringen beslutade i april 2004 direktiv till en parlamentarisk kommitté, Integritetsskyddskommittén (Ju 2004:05), med uppdrag att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten, att överväga om regeringsformens bestämmelse om skydd för den personliga integriteten i 2 kap. 3 § andra stycket borde ändras samt att överväga om det vid sidan av befintlig lagstiftning borde finnas generellt tillämpliga bestämmelser till skydd för den personliga integriteten. Kartläggnings- och analysuppdraget redovisades i betänkandet Skyddet för den personliga integriteten – Kartläggning och analys (SOU 2007:22). I sitt slutbetänkande Skyddet för den personliga integriteten – Bedömningar och förslag (SOU 2008:3) redovisade kommittén bl.a. förslag till ett stärkt grundlagsskydd för den personliga integriteten och ett förslag om straff för viss fotografering och filmning. Betänkandets förslag har hittills lett till införandet av bestämmelsen i 2 kap. 6 § andra stycket RF (prop. 2009/10:80, bet. 2009/10:KU19, rskr. 2009/10:304, bet. 2010/11:KU4, rskr. 2010/11:21) och till införande av ett nytt brott i 4 kap. brottsbalken, kränkande fotografering (prop. 2012/13:69, bet. 2012/13:JuU21, rskr. 2012/13:250).

I sitt slutbetänkande framhöll Integritetsskyddskommittén att det finns mycket som talar för att det i Sverige borde inrättas en ordning som innebär att regeringen genom en skrivelse årligen informerar riksdagen om utvecklingen i fråga om integritetsskyddet (SOU 2008:3 s. 326). Kommittén ansåg också att det fanns skäl att överväga en utveckling och breddning av Datainspektionens funktioner. Kommittén ansåg att uppgiften inte borde vara begränsad till området för elektroniska data eller till teknikutvecklingen som sådan utan omfatta också teknikens tillämpning i människornas vardag (bet. s. 332). Vidare bedömde kommittén att det kunde finnas skäl att i en framtid överväga inrättandet av ett särskilt integritetsskyddsråd med ett brett uppdrag att vaka över integritetsskyddet i dess helhet (bet. s. 335).

Senare års utveckling

Historiskt sett har det konstitutionella skyddet för den personliga integriteten – vid sidan av skyddet för den kroppsliga integriteten – i allt väsentligt inskränkt sig till att begränsa det allmännas utrymme att ingripa mot den fria åsiktsbildningen som en av grundvalarna för ett demokratiskt styrelseskick (prop. 2009/10:80 s. 176). Rättsutvecklingen under senare år visar dock att synen på skyddet för enskildas privatliv har förändrats och att detta intresse numera betonas starkare än tidigare. I förarbetena till 2 kap. 6 § andra stycket RF framhålls att respekten för individens självbestämmande är grundläggande i en demokrati (prop. 2009/10:80 s. 176). Förstärkningen av grundlagsskyddet för den personliga integriteten innebär således att vikten av individens självbestämmande nu betonas tydligare än tidigare i grundlag.

Frågor som rör skyddet för den personliga integriteten har vidare under senare år fått förhållandevis stort utrymme i den allmänna debatten om statens möjligheter att använda olika tekniska hjälpmedel i syfte att förebygga, utreda och lagföra brott. Detta gäller t.ex. i fråga om möjligheterna att använda hemlig rumsavlyssning (s.k. buggning) och hemlig övervakning och avlyssning av elektronisk kommunikation samt lagring av trafikdata från mobiltrafik och internetanvändning för brottsbekämpande syften. Signalspaning i försvarsunderrättelseverksamhet är ett annat område som har varit

föremål för debatt. Frågor om skydd för den personliga integriteten har i denna lagstiftning varit grundläggande för ett system med tydliga tillstånds- och kontrollmekanismer.

Enskildas användning av internet har ökat stadigt under hela 2000-talet. Den mängd information som är tillgänglig på internet har ökat explosionsartat. Den är lättillgänglig – bl.a. genom användning av effektiva sökmotorer – och i stor utsträckning helt kostnadsfri. En betydande del av informationen har också tillkommit genom enskildas användning av internet, snarare än genom traditionella mediekanaler.

Alla myndigheter använder i dag informationsteknik. I princip all framställning av information hos myndigheterna sker på elektronisk väg och utbyte av uppgifter mellan myndigheter sker i stor utsträckning elektroniskt. Ett omfattande förvaltningspolitiskt reformarbete pågår i syfte att effektivisera förvaltningen bl.a. genom att utveckla den s.k. elektroniska förvaltningen (e-förvaltning).

Integritetsrisker i både offentlig och privat verksamhet

Enskilda har ofta små möjligheter att påverka vilka uppgifter som statliga och kommunala myndigheter får tillgång till om dem själva. Hanteringen av informationen sker vanligen på villkor som utesluter den enskildes inflytande över vilka uppgifter som behandlas. Möjligheterna att få uppgifter raderade är normalt sett mycket begränsade när uppgifterna förekommer i allmänna handlingar. Den mängd av uppgifter som totalt sett förekommer i verksamheten är också mycket stor. Det är mot bakgrund av detta viktigt att säkerställa respekten för den personliga integriteten inom ramen för den verksamhet som det allmänna ansvarar för.

Regeringens ambition är att Sverige ska vara en av de ledande nationerna i världen när det gäller e-förvaltning. En väl fungerande e-förvaltning kan både bidra till en effektiv hushållning med statens medel och erbjuda medborgarna en hög servicenivå i kontakterna med myndigheterna. Tekniska lösningar som tas fram inom e-förvaltningsarbetet kan bidra till att skyddet för den personliga integriteten stärks, bl.a. genom att de personuppgifter som myndigheterna har att hantera i sina verksamheter hålls korrekta och aktuella. En del integritetsrisker kan också minimeras genom god användning av tek-

niska lösningar för säkert informationsutbyte mellan myndigheter. E-legitimation kan användas för att öka spårbarheten i sökningar. En ökad samordning av myndigheternas informationshantering kan dock samtidigt innebära ökade integritetsrisker. Motsvarande risker kan även uppkomma när privata företag utvecklar affärsprocesser och samordnar sin datalagring.

Det samlade intrång i den skyddade personliga sfären som uppkommer som en följd av olika åtgärder, processer och övervakning som enskilda utsätts för i dagens samhälle är inte bara ett resultat av verksamhet som det allmänna ansvarar för. Enskilda utsätts i hög grad även för intrång i den personliga integriteten från andra enskilda. Användningen av internet som kanal för informationsspridning har skapat tidigare oanade möjligheter att utnyttja yttrandefriheten för att nå ut till andra med tankar och idéer eller med information som kan väcka debatt i viktiga samhällsfrågor. Men internet kan också användas av dem som vill sprida information i vida kretsar i syfte att skada andra. Personuppgifter som är lättillgängliga på internet kan också användas i bedrägligt syfte genom identitetsstölder och liknande. Tillgången till information kan även leda till särskilda risker för individer som har ett behov av skydd för sina personuppgifter på grund av att det finns en fara för att de utsätts för trakasserier, hot och våld.

Inom arbetslivet gäller att en arbetsgivare har rätt att, inom ramen för anställningsavtalet, bestämma bl.a. vilka åtgärder som ingår i arbetsuppgiften, hur arbetet ska utföras och var detta ska ske. En arbetstagare måste i princip följa en arbetsledningsorder, i vart fall så länge den anvisade åtgärden inte strider mot lag eller god sed på arbetsmarknaden eller annars är att anse som otillbörlig. Det innebär bl.a. att en arbetstagare i viss utsträckning kan behöva finna sig i att godta en övervaknings- eller kontrollåtgärd från arbetsgivarens sida. För att bedöma vad som är god sed när det gäller utövandet av kontrollåtgärder måste dock normalt en avvägning göras mellan arbetsgivarens intresse av åtgärden och arbetstagarens intresse av skydd för den personliga integriteten. Åtgärden kan vara tillåtlig på denna grund bara om den är proportionerlig i förhållande till sitt syfte.

Överenskommelse om en ny utredning

Hösten 2011 träffades mellan regeringen och Socialdemokraterna en överenskommelse om att tillsätta en parlamentarisk integritetskommission. Enligt överenskommelsen ska kommissionen ha ett uppdrag som löper under längre tid och som har ett tydligt individperspektiv. Kommissionen ska enligt överenskommelsen beakta olika former av integritetsaspekter, bl.a. sådana som kan förekomma inom sociala medier, privata företag och förvaltningsmyndigheter. Den ska också följa upp de överväganden Integritetsskyddskommittén gjorde när det gäller behovet av att inrätta ett integritetsskyddsråd.

Uppdraget att kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten

Möjligheterna att via internet snabbt sprida information om företeelser i omvärlden eller att dela information om egna tankar och idéer med en stor krets människor skapar ovärderliga möjligheter för enskilda att utnyttja sin informations- och yttrandefrihet. Stora mängder data kan nu överföras på mycket kort tid. Den snabba tekniska utvecklingen på it-området har bidragit till detta. Samtidigt har kostnaderna för denna hantering minskat, vilket gör att såväl myndigheter som privata företag sett möjligheter till nya sätt att bedriva och effektivisera sin verksamhet. I detta ingår exempelvis kartläggning av enskildas beteendemönster på internet för att skapa nya affärsmöjligheter. Även om ett visst företag inte har tekniska eller administrativa möjligheter att göra detta i egen regi finns det företag som säljer tjänster som ger tillgång till beräkningskapacitet, datalagring och analysfunktioner över internet, s.k. molntjänster. De nya möjligheterna innebär samtidigt nya utmaningar och risker bland annat för intrång i den personliga integriteten.

Enskilda använder i stor utsträckning sociala medier, t.ex. Facebook, Instagram och Twitter, där de offentliggör potentiellt integritetskänsligt material som kan få stor och oförutsedd spridning. Det kan vara svårt för enskilda att bilda sig en uppfattning om omfattningen av behandlingen av deras personliga uppgifter efter sådan publicering och spridning. Detta väcker frågor bl.a. om vem som har rätt till uppgifterna när de väl har publicerats och hur enskilda bör gå till väga om de önskar få dem borttagna.

Integritetsskyddskommittén (Ju 2004:05) redovisade i betänkandet Skyddet för den personliga integriteten – Kartläggning och analys (SOU 2007:22) en omfattande kartläggning och analys av sådan lagstiftning som berör den personliga integriteten. Uppdraget utfördes utifrån ett utpräglat lagstiftningsperspektiv. Vidare omfattade kartläggningen och analysen endast sådan verksamhet som bedrivs enbart av det allmänna eller av både det allmänna och enskilda, t.ex. skola, sjukvård, och forskning, och inte sådan verksamhet som i första hand endast bedrivs av enskilda aktörer. Någon mer ingående undersökning av vad senare års teknikutveckling och teknikanvändning som helhet inneburit i fråga om riskerna för integritetsintrång för enskilda individer har inte gjorts.

Mot bakgrund av samhälls- och teknikutvecklingen under senare år finns nu behov av att genomföra en kartläggning och analys av sådana faktiska eller potentiella risker för intrång i den personliga integriteten som kan finnas vid användning av informationsteknik i både privat och offentlig verksamhet. En sådan kartläggning bör göras med utgångspunkt i ett tydligt individperspektiv. I detta ligger att alla slags åtgärder som kan påverka enskilda individer från integritetssynpunkt bör kartläggas. Att kartläggningen ska göras utifrån ett utpräglat individperspektiv innebär också att kommittén bör analysera riskerna för intrång i den personliga integriteten på ett samlat sätt ur den enskildes synvinkel och att bedömningarna inte begränsas till att enbart avse tydligt avgränsade verksamheter eller situationer. I det sammanhanget bör särskilt beaktas vilka möjligheter privatpersoner har att själva bestämma över hur information om dem används och vidareförmedlas för användning i annan verksamhet än den ursprungligen är avsedd för.

Inom ramen för kartläggningen bör en uppföljning göras av hur den reform av grundlagsskyddet för den personliga integriteten, som trädde i kraft 2011, har fallit ut. Uppföljningen bör innefatta en kartläggning och analys av de integritetsaspekter som aktualiserats i lagstiftningsarbetet sedan den nya grundlagsbestämmelsen trädde i kraft. Om kommittén med anledning av vad den kommer fram till i sin kartläggning och analys bedömer att det finns behov av att kartlägga och analysera även sådan lagstiftning som tillkommit dessförinnan kan kommittén förorda tilläggsdirektiv. I analysen av de potentiella riskerna för intrång i den personliga integriteten vid

användningen av modern informationsteknik bör hänsyn även tas till de fördelar som användningen av sådan teknik kan ha i både offentlig och privat verksamhet.

Uppdraget

Kommittén ska utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan finnas i samband med användning av informationsteknik. Kommittén ska vid kartläggningen och analysen beakta risker för intrång genom åtgärder såväl från andra individer och företag som från det allmännas sida. I uppdraget ingår att belysa eventuella skillnader ur ett könsperspektiv. Inom ramen för kartläggningen ska kommittén även följa upp och analysera effekterna i lagstiftningsarbetet av den förstärkning av grundlagsskyddet för den personliga integriteten som skedde genom lagstiftning som trädde i kraft 2011.

Uppdraget att överväga inrättandet av ett integritetsskyddsråd

Det finns för närvarande en rad myndigheter som har till uppgift att tillvarata enskildas intresse av skydd för den personliga integriteten. Datainspektionen har det övergripande ansvaret att värna skyddet för enskilda vid behandling av personuppgifter. Inspektionen har också ett övergripande tillsynsansvar när det gäller kameraövervakning enligt kameraövervakningslagen (2013:460). Även länsstyrelserna har ansvar för tillsyn över kameraövervakning, men det ansvaret begränsar sig till övervakning på platser dit allmänheten har tillträde. Post- och telestyrelsen har i uppdrag att utöva tillsyn vid behandling av uppgifter vid elektronisk kommunikation. Tillsyn över behandlingen av personuppgifter utövas på vissa särskilda områden även av andra myndigheter. Det finns inte något enskilt statligt organ som har ett bredare och mera övergripande uppdrag att följa utvecklingen på integritetsskyddsområdet.

Regeringen anser att det, i linje med vad Integritetsskyddskommittén tidigare framfört (SOU 2008:3 s. 335), nu finns anledning att överväga och ta ställning till värdet och behovet av att ge en myndighet ett brett och samlat uppdrag att följa utvecklingen på om-

rådet för den personliga integriteten. Om ett sådant behov bedöms finnas ska kommittén överväga om det är lämpligast att för detta ändamål inrätta ett särskilt integritetsskyddsråd eller om ett sådant uppdrag i stället bör anförtros en befintlig myndighet. Kommittén ska föreslå en lösning som är så kostnadseffektiv som möjligt och där överlappande ansvar och dubbelarbete i möjligaste mån undviks.

Vid sina överväganden ska kommittén beakta samhälls- och teknikutvecklingen i stort, särskilt de faktiska och potentiella risker för intrång i den personliga integriteten som kommitténs uppdrag omfattar.

Uppdraget

Kommittén ska, med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av sitt kartläggnings- och analysuppdrag följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd och särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet, samt föreslå nödvändiga författningsändringar.

Uppdragets genomförande och konsekvensbeskrivningar

Kommittén ska följa samhällsdebatten på integritetsskyddsområdet och bedriva sitt arbete utåtriktat och inhämta synpunkter från berörda intressenter i samhället, t.ex. genom att anordna hearings. Kommittén ska samråda med E-delegationen (Fi 2009:01), Datainspektionen, Post- och telestyrelsen och andra berörda myndigheter samt med arbetsmarknadens parter och med andra berörda organisationer. I sitt arbete ska kommittén följa utvecklingen av förhandlingarna inom EU med reformeringen av den unionsrättsliga dataskyddsregleringen. Kommittén ska även följa arbetet inom Regeringskansliet med de förslag som Utredningen om registerutdrag i arbetslivet (A 20013:04) senare kommer att redovisa för regeringen (dir. 2014:34).

Inom Regeringskansliet pågår ett arbete med att se över den straffrättsliga lagstiftning som syftar till att skydda enskilda mot hot och andra fridskränkningar bl.a. på internet. Kommittén ska följa hur detta arbete fortlöper.

Om regeringen beslutar att ge en utredning i uppdrag att utreda frågor med anknytning till kommitténs uppdrag att överväga frågor som rör den personliga integriteten, ska kommittén samråda med den utredningen.

I uppdraget ingår inte att föreslå ändringar i grundlag.

Kommittén ska i enlighet med vad som föreskrivs i kommittéförordningen (1998:1474) redovisa konsekvenserna av sina förslag och vid behov föreslå hur dessa ska finansieras.

Redovisning av uppdraget

Uppdraget ska redovisas slutligt senast den 1 december 2016. Kommittén får, om den bedömer att det är lämpligt, lämna ett eller flera delbetänkanden.

(Justitiedepartementet)

Kommittédirektiv 2016:12

Tilläggsdirektiv till Integritetskommittén (Ju 2014:09)

Beslut vid regeringssammanträde den 18 februari 2016

Förlängd tid för och ändring av uppdraget

Regeringen beslutade den 8 maj 2014 kommittédirektiv om den personliga integriteten (dir. 2014:65). I uppdraget ingår bl.a. att utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet och att, med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av kartläggnings- och analysuppdraget, följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd. Enligt utredningens direktiv skulle uppdraget redovisas senast den 1 december 2016.

Utredningstiden förlängs. Uppdraget ska i stället redovisa ett delbetänkande senast den 31 maj 2016 som omfattar dels kartläggningen och analysen av riskerna för integritetsintrång, dels behovet av att inrätta ett integritetsskyddsråd. Uppdraget i övrigt ska redovisas senast den 1 juni 2017.

(Justitiedepartementet)

kirei

PM

29 oktober 2015

Integritetskommittén (Ju 2014:09)
Kirei 2015:20

Integritetsskyddande teknik

Innehåll

1 Rätten till ett privatliv 5
1.1 Individens egna val 6
1.2 Samhällets ansvar 7
1.3 Teknikens roll 8

2 Integritetsskyddande teknik 11
2.1 Informationssäkerhet och skydd för privatlivet 11
2.2 Koncentrerade respektive distribuerade informationskällor 11
2.3 Säker identifiering med bibehållen spårbarhet 12
2.4 Blinda elektroniska underskrifter 14
2.5 Integritetsbevarande informationsutvinning 16

3 Inbyggt integritetsskydd 21
3.1 Uppgiftsminimering 24
3.2 Informerat medgivande 25
3.3 Transparens 27
3.4 Förebyggande verifierbart skydd 28
3.5 Möjlighet att återta ett medgivande 29

4 Ett ledningssystem för persondataskydd 31

5 Referenser 33

1 Rätten till ett privatliv

Många tjänster i vardagen som vilar på modern informationsteknik, och som uppfattas som oumbärliga, medför inte sällan en ingående kartläggning av individen. Exempel på teknik som medför sådan kartläggning innefattar att bära med sig en mobiltelefon, att köra en bil av nyare snitt eller att använda ett betalkort för sina vardagliga inköp. Resor med kollektivtrafik företas även företrädesvis med ett kontaktlöst resekort med en identitet som registreras och kan spåras.

Utöver detta väljer många att använda sociala medier och söktjänster på internet, som tillhandahålls av leverantörer vars själva affärsidé går ut på att kartlägga individen för att sedan dra nytta av denna kunskap genom till exempel riktad annonsering.

Med tiden tenderar även fler och fler informationskällor uppstå som påför ytterligare dimensioner i kartläggningen av individen. Elmätaren i varje hem är idag uppkopplad och registrerar i praktiken vanorna i hushållet; från när någon går upp på morgonen och slår på kaffebryggaren, när det duschas och tappvarmvatten bereds, till när man kommer hem och senare går och lägger sig och släcker ljuset.

Det går knappast som enskild medborgare att värja sig mot det integritetsintrång som sker genom användning av dessa tekniker, med mindre än att aktivt välja att inte använda flertalet av dem. Få kan nog tänka sig att sluta köpa elektricitet eller att sluta använda en mobiltelefon. Alternativen, att som konsument försöka skydda sin privata sfär genom olika medel, blir ofta så opraktiskt och kostsamt att det aldrig står som ett reellt alternativ för andra än grovt kriminella. Denna grupp av individer kan tänkas vidta långtgående åtgärder för att undvika att lämna elektroniska fotspår, innefattande att uteslutande använda kontanter, att alltid bruka anonymiseringstjänster på internet och oregelbundet byta mellan olika mobiltelefoner och oregistrerade SIM-kort på olika platser, och också hålla apparaterna avstängda då de inte behövs.

Det alternativ som i övrigt står till buds är att de informationstjänster vi använder i vardagen görs säkra från ett persondataskyddsperspektiv. Denna skrift belyser sådana tekniska, administrativa och organisatoriska åtgärder som kan vidtas för att främja skyddet av privatlivet. Skriften har betydande fokus på informationsutvinning ur stora känsliga uppgiftskällor, men också på hur det kan undvikas att sådana känsliga uppgiftskällor uppstår som sidoeffekt av något annat.

1.1 Individens egna val

Individens egna möjligheter att påverka skyddet av sin privata sfär visavi den kartläggning som följer av vardagen, är som tidigare nämnts begränsad och synnerligen omständlig. Anonymiseringstjänster på internet kan skydda kommunikationen så att den blir mycket svår att härleda till en internetadress. Men de uppgifter en individ i övrigt sprider genom långvarig användning av informationstjänster ger som regel ändå tillräckligt med information för att unikt kunna identifiera denna person bland andra.

De individer som inte önskar få sina intressen, farhågor och åkommor kartlagda måste på ett mycket medvetet sätt avstå ifrån att i någon betydande utsträckning använda till exempel sociala medier. Det är emellertid inte endast den information som användaren lämnar ifrån sig i form av direkta personuppgifter, bilder eller berättelser som kan användas för kartläggning. Minst lika mycket information kommer av vilka vänner man har, vilka länkar man klickar på, vilka sidor man gillar, vilka nätverk man ansluter ifrån, et cetera. Även de populära söktjänsterna innebär motsvarande kartläggning. I detta korreleras sökord med andra tjänster som tillhandahålls av leverantören. Ett sådant exempel är analys av besökstrafik på webbsidor. Mot att webbplatsinnehavaren tillhandahålls ett verktyg för besöksstatistik, får leverantören av söktjänsten del av samma uppgifter, som vidare kan korsrefereras mot varje individuell användare. Dessa uppgifter, som när de sammanställs unikt identifierar en person bland andra, kallas *kvasi-identifierare*.

För att undvika sådan kartläggning krävs av den enskilde användaren en betydande kunskap om hur denne ska skydda det egna privatlivet. Det fordras bland annat särskilda insticksprogram i webbläsaren för att på ett bra sätt blockera funktioner som används för

spårning. Vidare, när sökning efter information sker som på något sätt avslöjar omständigheter som individen önskar hålla för sig själv behöver anonymiseringsteknik användas[1] som tvättar kommunikationen från uppgifter som annars kan relateras till användaren, till exempel den internetadress som används och det elektroniska fotavtryck webbläsaren normalt efterlämnar sig.

Men även för de som vidtar sådana åtgärder kommer användningen av informationsteknik i vardagen och i arbetslivet i praktiken innebära en ingående kartläggning som svårligen kan undvikas. Avgörande för skyddet av den privata sfären blir då om, och i så fall på vilket sätt, sådana uppgifter kan samköras inom eller mellan dessa informationskällor. De strukturerade och stora informationskällorna (*"big data"*) blir därmed också de som innebär de största riskerna för den enskildes personliga integritet.

1.2 Samhällets ansvar

I Sverige finns en stark kultur och tradition med tillit till statsapparaten, något som möjligen inte kan sägas gälla i alla av våra grannländer. Inom Europa och EU finns ett antal nationer med miljontals människor som i modern tid upplevt förtryckande regimer och svåra övergrepp, och där det därför också finns en stark skepticism bland befolkningen kring kartläggning och registrering av medborgaren. Därmed förs också integritetsdebatten i en annan ton i till exempel Tyskland jämfört med Sverige. Tyskland har en av Europas starkaste persondataskyddslagstiftningar, och är ett av de länder inom EU där man tidigt funnit att datalagringsdirektivet står i strid med konstitutionen, och där man också rivit upp den nationella lagstiftningen kring detta.

Den samhällsdebatt som förs i Sverige förefaller dock inte ha lett till någon generellt förändrad inställning till integritetsfrågorna bland medborgarna, i vart fall inte än. Samtidigt synes det existera, bland åtminstone en minoritet av befolkningen, en tilltagande oro över den registrering som sker. Den allmänna bristen på transpa-

[1] Till exempel TOR-browser:
`https://www.torproject.org/projects/torbrowser.html`

rens och känslan av att vadhelst man företar sig efterlämnar elektroniska fotspår kan förväntas vara bidragande orsaker, inte minst bland personer mot vilka det existerar en reell hotbild.

Denna oro kan vara mer eller mindre befogad, men så länge uppgifterna existerar finns ingen absolut säkerhet kring att de inte kan röjas och missbrukas. Att stora informationsläckage med viss regelbundenhet uppmärksammas i massmedia torde också öka medvetenheten om riskerna bland medborgarna.

Utifrån en strikt holistisk vy är det dock i dagsläget svårt att se att det finns tillräckligt starka kommersiella drivkrafter för att effektiva integritetsskyddande tekniker ska utvecklas och införas på bred front inom den privata sektorn. Snarare synes informationskällor innehållande stora mängder personuppgifter många gånger betraktas som en värdefull tillgång inom en organisation.

Det kan därför knappast förutsättas att privata företag på egen hand och i stor skala går i bräschen för att införa integritetsskyddande tekniker på ett sätt som försvårar, fördyrar eller på annat sätt försvagar företagets ställning gentemot dess konkurrenter. Att det uppstår en ökad medvetenhet bland medborgarna kring riskerna med registreringen av de digitala fotspåren är emellertid till nytta för hela samhället, och en nödvändighet för att vårt uppkopplade liv ska kunna fortsätta utvecklas.

För att inte denna utveckling i förlängningen ska leda till ohållbara risker för den personliga integriteten är det troligt att frågan i högre grad än nu måste drivas av det allmänna. Myndigheter och offentligt styrda bolag utgör en viktig länk i att öka medvetenheten genom att föregå med goda exempel och visa vad kunder och medborgare bör förvänta sig i sina elektroniska relationer. Allt eftersom medvetenheten ökar bland konsumenter kan den affärsmöjlighet förväntas uppstå, som leder till att smarta integritetsskyddande tekniker blir ett konkurrensmedel som kan stärka ett företags ställning snarare än att försvaga den.

1.3 Teknikens roll

Graden av skydd av den privata sfären framställs ofta som en avvägning mellan olika motstående intressen, till exempel intresset av att på ett effektivt sätt kunna upptäcka och utreda brottslig verksamhet - ställt mot de frihetliga rättigheterna. Men genom väl utformad

integritetsfrämjande teknik kan det emellertid gå att uppnå en mer fördelaktig jämvikt mellan dessa intressen. Med det avses att möjligheten till spårbarhet kanske kan tillvaratas, samtidigt som ett effektivt skydd för den privata sfären utformas.

Integritetsskyddande tekniker behöver därför inte betyda fullständig anonymitet och ospårbarhet, men kan kräva att flera aktörer med ansvar för olika informationskällor samverkar för att klarlägga ett visst förlopp. Känsliga uppgifter i ett register kan kopplas till pseudonyma identifierare, istället för direkta identifierare som till exempel personnummer. Dessa pseudonyma identifierare avses vara olänkbara mellan olika sammanhang, vilket medför att uppgifter i skilda register inte enkelt kan kopplas samman utan att en *delvis betrodd* mellanhand tillhandahåller en sådan koppling. Exempel på en sådan tillämpning finns i avsnitt 2.3.

På så sätt kan en administrativ eller organisatorisk separation åstadkommas, som kräver att flera aktörer samverkar kring att sätta samman den kompletta bilden av en person eller ett händelseförlopp. Dessa *delvis betrodda* mellanhänder behöver emellertid inte vara del i de faktiska händelsekedjorna, och har inte heller samtliga de pusselbitar som krävs för en kartläggning. Vid till exempel en polisiär utredning behöver mellanhanden många gånger inte ens känna till vilken information som eftersöks. I det följande visas på ett antal olika principer och kombinationer av tekniska, administrativa och organisatoriska åtgärder som kan användas för att åstadkomma ett effektivt skydd för privatlivet, samtidigt som intresset av användbarhet, kostnadseffektivitet och spårbarhet omhändertas.

2 Integritetsskyddande teknik

2.1 Informationssäkerhet och skydd för privatlivet

Informationssäkerhet och teknik som ger skydd för privatlivet kan sägas vara två olika grenar inom persondataskyddet. Då personuppgifter som behandlas i ett system ska skyddas inrättas vanligen olika former av informationssäkerhetskontroller, som i enlighet med gällande lagstiftning ska svara upp mot de risker som behandlingen av uppgifterna medför.

Skydd av privatlivet med integritetsskyddande teknik kan emellertid utformas på sådant sätt att vissa risker aldrig ens uppstår, bland annat enligt principerna för *inbyggt integritetsskydd* som diskuteras i nästa kapitel. Den avgörande skillnaden mellan dessa två grenar är att integritetsskyddande teknik många gånger gör det möjligt att förvissa sig om effektiviteten i skyddet för privatlivet, på ett verifierbart och transparent sätt.

Informationssäkerhetskontroller kan förvisso försvåra att uppgifter röjs till obehöriga, men de erbjuder sällan absolut säkerhet på sådant sätt att de inte kan kringgås, eller helt enkelt fallera. Det är många gånger också svårt att verifiera kontrollernas effektivitet och att skapa transparens i detta avseende. Ett effektivt skydd för privatlivet består därför i samverkande åtgärder inom båda dessa grenar.

2.2 Koncentrerade respektive distribuerade informationskällor

Att uppgifter inte finns samlat hos en aktör i en strukturerad och enkelt sökbar form innebär i sig ett visst skydd mot intrång i den

privata sfären. Det existerar idag till exempel ett oräkneligt antal övervakningskameror i urbana miljöer där allmänheten vistas - i butiker och restauranger, på torg och på arbetsplatser. Hade samtliga bilder samlats in i ett centralt system där de kunde analyseras och samköras hade riskerna för svåra integritetsintrång blivit långt mycket större än då informationen är distribuerad över många olika aktörer med eget ansvar för den egna information, och där det krävs betydande ansträngningar för att samla in och sammanställa uppgifterna. För brottsutredande ändamål kan emellertid den polisiära myndigheten besöka de aktörer som kan tänkas ha material som är intressant i en utredning, för att begära tillgång till just de aktuella bilderna. De enskilda aktörernas bilder är i sig möjligen inte särskilt intressanta var och en för sig, men då flera aktörers material sammanställs och korreleras träder en mer komplett bild fram.

Ett sådant arbetssätt fordrar förstås större resurser, men det illustrerar väl hur riskerna minskar då uppgifter hålls isär, samtidigt som spårbarheten bibehålls. På samma sätt minskar riskerna om till exempel olika myndigheters register kan hållas isär, och att det krävs flera olika aktörer som samverkar för att forma den kompletta bilden.

2.3 Säker identifiering med bibehållen spårbarhet

Det finns inget motsatsförhållande mellan att säkert identifiera en person och att samtidigt låta denne använda en tjänst eller ett system under pseudonym. Måste till exempel en prenumerant på en elektronisk utgåva av en tidning identifieras med namn och adress? Troligen inte. Samtidigt är det kanske önskvärt att säkerställa att vederbörande efterlever de villkor som följer av tjänsten, till exempel att inte vidaredistribuera utgåvorna eller följa *netiketten* som gäller för diskussionsforumen.

Detta kan realiseras genom att använda intygsbaserad identifiering, innebärande att den enskilde legitimerar sig mot en utställare av identitetsintyg. Identitetsintygets innehåll kan variera beroende på vad som krävs för den aktuella tjänsten till vilken användaren söker åtkomst. I dess enklaste form tillhandahålls endast en beständig pseudonym identifierare, som är unik för relationen mellan användaren och tjänstetillhandahållaren. Mellan olika tjänstetillhandahållare varierar den pseudonyma identifieraren på ett sådant sätt att två tjänstetillhandahållare inte kan samköra sina register för att finna användare

som förekommer i dem båda.

Identitetsintyget kan också bära attribut som relaterar till användaren, till exempel att innehavaren av intyget är över 18 år, har en viss kreditvärdighet eller innehar viss juridisk behörighet. Den typen av uppgifter kan ligga till grund för en *attributbaserad åtkomstkontroll* som kan användas utan att för den sakens skull behandla namn, personnummer, kön, et cetera. Ett konkret exempel på användning av sådan teknik idag är inom *Skolfederation*[1], där elever genom SAML-protokollet[2] kan identifieras som tillhörande en viss skola och viss kurs för att kunna ta del av digitala läromedel. Leverantören av läromedlen får dock aldrig del av några andra personuppgifter som relaterar till eleven.

Även infrastrukturen för Svensk e-legitimation bygger på samma teknik. De e-tjänster som myndigheter tillhandahåller idag är emellertid utformade på ett sådant sätt att personnummer alltid måste förmedlas för att ge rätt behörighet. Det finns dock inga hinder att utveckla användningen av tekniken i detta avseende och minska beroendet till personnumret. Det är också fullt möjligt att använda attributbaserad åtkomstkontroll inom samma infrastruktur, fristående eller tillsammans med pseudonyma eller direkta identifierare.

Spårbarhet vid pseudonym identifiering säkerställs genom att den part som ställt ut intyget kan tillhandahålla länken mellan pseudonymen och den faktiska identiteten. Denna aktör blir i en sådan modell den *delvis betrodda* part, som tillsammans med tjänstetillhandahållaren kan sammanlänka en person med en transaktion.

Verksamheten som utställare av identitetsintyg till allmänheten kan emellertid behöva regleras på sådant sätt att det inte från dennes händelsehistorik går att utläsa vem som besökt vilken e-tjänst och när. Detta bör kunna åstadkommas civilrättsligt genom de avtal som tecknas inom respektive identitetsfederation. Om utställaren av intyget sparar intygets elektroniska stämpel kan kopplingen återskapas tillsammans med en tjänstetillhandahållare, givet att denne

[1] `https://www.skolfederation.se/`

[2] *Security Assertion Markup Language* är ett dataformat för att utbyta identifiering- och behörighetsinformation mellan två parter – vanligen mellan identitetsleverantören och tjänsteleverantören.

sparat det intyg mot vilket åtkomst beviljades. På så sätt krävs båda dessa aktörer i samverkan för att klarlägga en sådan händelsekedja.

2.4 Blinda elektroniska underskrifter

Ett annat teknikområde av betydelse i integritetsbevarande sammanhang är så kallade *blinda* elektroniska underskrifter. Med det avses att signatären, den som skriver under en handling, kan göra det utan att ta del av innehållet i handlingen. Det är också möjligt att selektivt låta signatären ta del av vissa valda delar av handlingen som skrivs under, medan andra delar döljs. Tekniken och principerna för blinda elektroniska underskrifter har existerat i närmare 30 år, men är nu föremål för standardisering inom *International Organization for Standardization* (ISO) och *the International Electrotechnical Commission* (IEC) genom serien ISO/IEC 18370.

Sådana blinda elektroniska underskrifter har flera tillämpningsområden som integritetsskyddande teknik. Bland annat är det möjligt att åstadkomma ett elektroniskt röstningsförfarande, där det är säkerställt att endast röstberättigade har möjlighet att rösta (och att endast avlägga så många röster denne är berättigad till) samtidigt som det i efterhand inte är möjligt att härleda vem som lagt vilken röst.

Förenklat kan det sägas att varje röstberättigad framställer sin egna unika röstsedel innehållande det val den röstberättigade avser avlägga, och får denna röstsedel certifierad som äkta av signatären utan att avslöja några unika egenskaper kring innehållet i röstsedeln. Alla insamlade elektroniska röstsedlar kan verifieras som äkta och att innehållet inte manipulerats, men endast den som framställde röstsedeln kan peka ut vilken den är bland de andra.

Med utgångspunkt i samma teknik är det möjligt att framställa elektroniska pengar. Med elektroniska pengar avses ett elektroniskt förvarat penningvärde som godtas som betalningsmedel gentemot andra än utgivaren. I Sverige finns ett juridiskt ramverk genom lagen om elektroniska pengar (2011:755) som trädde i kraft 1 juli 2011.

Blinda elektroniska underskrifter kan användas för att på kryptografisk väg åstadkomma elektroniska sedlar[3] som individen kan bära med sig på ett kort eller i sin mobiltelefon, och som inte kan spåras på ett sådant sätt att det går att kartlägga hur individen spenderat sitt innehav. Däremot kan individen tillsammans med utställaren avgöra vem som löst in en viss elektronisk sedel, och även spärra

sådana elektroniska kontanter som gått förlorade. Därvid kvarstår även möjligheterna att utreda och förhindra bedrägerier och stölder.

Individens anonymitet i spenderandet av de elektroniska pengarna garanteras så länge vederbörande inte försöker dubbelspendera en utställd elektronisk sedel. Skulle så ske kommer tillräckligt med information avslöjas om individens elektroniska plånbok att denne kan spåras och hållas ansvarig. Det kan därför också sägas kräva ungefär samma form av tillit till mottagaren av betalningen som för betalningar med betalkort.

I en utvidgning av konceptet kan de elektroniska sedlarna ersättas med elektroniska checkar av visst maximalt värde. På så sätt förenklas betalningarna så att beloppet alltid blir jämt, och eventuella utmaningar kring elektronisk växel som ska föras tillbaka till individens plånbok kan elimineras.

Tekniken i sig är möjligen tämligen komplicerad, men användningen av den är analog med den traditionella plånboken och sedlarna. Det torde också finnas en viss efterfrågan på säkrare elektroniska betalningsmedel. Undersökningar har visat att så många som 23% av konsumenterna som använder elektroniska betalningar är bekymrade över kartläggningsaspekten[4]. Ett område där elektroniska pengar också skulle kunna användas och medföra betydande positiva effekter är inom kollektivtrafikbranschen.

Att elektroniska fotspår uppstår i samband med resor som företas med en regional kollektivtrafikmyndighet är inte helt oproblematiskt, då många sannolikt inte har något reellt alternativ till att nyttja dessa tjänster för att klara vardagslivet. Enligt Regeringsformens (1974:152) 2 kap. 6 § 2 är det dock en grundläggande rättighet för var och en att inte bli övervakad eller kartlagd av det allmänna. Samtidigt finns ett starkt intresse av ett på ett säkert, snabbt och kontantlöst sätt kunna resa. Det har också under lång tid skissats på modeller för enkelt sömlöst resande mellan olika trafikslag och trafikleverantörer. Aktörernas skilda affärsmodeller, taxestrukturer och olika sätt att ta betalt har av branschen identifierats som hinder för ökat kollektivt resande[3].

En plånbok med elektroniska pengar förvarade i till exempel en

[3] http://www.samtrafiken.se/utvecklingssamverkan/projekt/gemensamma-biljett-och-betallosningar/

mobiltelefonen skulle kunna användas för att betala för resorna i det ögonblick resenären stiger ombord på ett fordon eller passerar en spärr, utan att behöva skaffa ett särskilt resekort eller för den sakens skull sätta sig in i de olika aktörernas taxor och biljettutbud.

Elektroniska pengar skulle kunna utgöra det alternativ med vilket man på ett säkert, snabbt och enkelt sätt kan betala för kollektivtrafikresor utan att en ingående kartläggning uppstår. Man skulle då också på ett naturligt sätt kunna vidga användningen av ett sådant betalningsmedel och erbjuda resenären andra typer av tjänster i anslutning till resan, kanske en kopp kaffe eller en frukost ombord på tåget.

2.5 Integritetsbevarande informationsutvinning

Det finns många goda orsaker till att kunna analysera stora mängder integritetskänsliga uppgifter. Det kan till exempel handla om forskningsändamål, för att kunna spåra smittspridning eller för att utreda brottslig verksamhet. Det kan dock många gånger vara problematiskt att öppna och samköra sådana informationskällor på grund av de risker som då uppstår. I sådana situationer kan integritetsskyddande tekniker erbjuda det skydd som krävs för att möjliggöra analysen. I detta avsnitt belyses några av de tekniker och tillvägagångssätt som kan nyttjas för sådan integritetsbevarande informationsutvinning.

2.5.1 Anonymisering

Effektiv anonymisering av uppgifter kan vara väsentligt svårare än vad det vid första anblicken förefaller. Det finns ett antal uppseendeväckande misstag som gjorts och som nått offentlighetens ljus. Ett av de mest omskrivna är tävligen *the Netflix Prize*, en tävling som iscensattes 2006 och som gick ut på att tävla om ta fram den bästa algoritmen för att förutse tittares betygsättning på filmer givet dennes preferenser (som kommit till uttryck genom betygsättning av andra filmer). Netflix publicerade som del i tävligen i anonymiserad form en databas över 100 miljoner betygsättningar som 500 000 kunder gjort, omfattande cirka 10% av det totala antalet betygsättningar som existerade. Två forskare vid University of Texas[5] visade emellertid att det fortfarande och utifrån tämligen begränsade kunskaper om en individ ändå gick att identifiera denne i unikt i databasen, och utifrån den

kunskapen utvinna känsliga uppgifter som till exempel vilka politiska åsikter personen syntes ha. Sårbarheten ligger i att det räcker att känna till endast ett fåtal filmer som en person tittat på och ungefär när i tiden detta har skett för att det ska gå att identifiera denne och röja hela dennes tittarhistorik.

En annan omskriven händelse som skedde ungefär samtidigt var då *America Online* (AOL) publicerade en databas över 20 miljoner internet-sökningar som 650 000 användare hade gjort över en tremånadersperiod. *The New York Times*[1] visade att det genom att korsreferera uppgifter från sökningarna med telefonkatalogen gick att röja identiteten på enskilda personer, och därmed avslöja hela deras sökhistorik.

Fallen är ett exempel på hur *kvasi-identifierare* kunnat användas för att härleda en individs riktiga identitet, även då alla direkta identifierare tagits bort och då betydande ansträngningar gjorts för att anonymisera, korta och även till viss del förvanska vissa uppgifter. Robust anonymisering utgår därför ifrån att göra det tillräckligt svårt att identifiera enskilda personer i en informationsmängd, då det sällan går att åstadkomma total anonymitet. Detta kräver dock vanligen att inte bara vissa attribut avlägsnas, utan även att de uppgifter som ska analyseras avpersonifieras. Detta kan åstadkommas genom krypterande anonymisering, vilket behandlas separat i avsnitt 2.5.3. Det kan också göras med hjälp av modifierande anonymisering, till exempel *k*-anonymisering eller slumpredigering.

K-anonymisering

K-anonymisering är en metod för att säkerställa att minst *k* personer identifieras av de attribut som återstår, där *k* är bestämt till ett tillräckligt robust gränsvärde för att riskerna ska anses vara acceptabla. Detta sker genom att generalisera återstående attribut. Generalisering innebär i detta sammanhang att attribut ersätts med andra som fortfarande är sanna. Ett postnummer kan översättas till ett ortsnamn för sämre noggrannhet, et cetera.

Slumpredigering

Slumpredigering (eller randomisering) bygger på att ett slumpmässigt brus påförs data som gör att aggregatet av datat ändå är tillräck-

ligt exakt för att analyseras statistiskt, men där varje post i sig är tillräckligt felaktig för att sakna värde.

Något förenklat skulle till exempel en forskare, som ska undersöka hur medborgarnas kroppslängd i olika ålderskategorier i medeltal varierar geografiskt för män respektive kvinnor, kunna ta del av ett register där uppgiften om kroppslängd slumpredigerats med $\pm$ 15 centimeter. För ett geografiskt område där underlaget i varje kategori består i åtminstone några hundratal invånare, kan det förväntas att det slumpmässigt påförda bruset på varje post i registret tar ut varandra så till den grad att en relevant medellängd för gruppen ändå kan beräknas. Samtidigt är uppgiften i varje enskild post så osäker att det kanske är tillräckligt svårt att identifiera enskilda individer i gruppen.

2.5.2 Maskininlärning

Maskininlärning är vad man inom området för artificiell intelligens brukar kalla statistiska metoder för regression eller klassificering. Regression är i sin tur en gren inom statistik där målet är att skapa en funktion som bäst passar observerade data. Maskininlärning ger förhållandet mellan observerade data och inlärda mönster, som erhållits genom att analysera stora mängder relevanta exempel.

Tekniken kan användas för att på maskinell väg identifiera vissa typer av mönster som uppstår inom en informationskälla, och klassificera denna observation enligt någon trovärdighetsgradering. Det skulle till exempel kunna användas för att i realtid analysera trafikuppgifter och lokaliseringsinformation för att upptäcka och förvarna inför huliganisters våldsangrepp och sammandrabbningar. Huliganer kan vara mer eller mindre vanliga individer som ibland samlas till arrangerade slagsmål. Dessa sammankomster torde föregås av vissa kommunikationsmönster och rörelser, som skulle kunna kännas igen genom sådan maskininlärning. Ett larm kan automatiskt genereras som påkallar polisens uppmärksamhet om att det med en viss procents sannolikhet kommer att uppstå ett slagsmål på en viss plats, varvid traditionellt polisarbete kan ta vid.

Från persondataskyddsperspektiv finns flera fördelar med maskininlärning. En analysen kan göras direkt i stunden och den stora merparten av uppgifter som inte bedöms som intressanta kan snabbt därefter gallras bort. Uppgifterna behöver inte analyseras av någon

människa, i vart fall inte innan det finns tydliga indikationer på att en viss händelse är nära förestående, och kanske inte ens då att något intrång behöver ske om det är händelsen och platsen i sig som är det intressanta i sammanhanget. Att uppgifterna inte behöver tillgängliggöras för någon människa minskar även risken för att de någon gång missbrukas.

Samtidigt bör det påpekas att maskininlärning är en mycket effektiv metod för att också urskilja enskilda individers användarmönster för att göra den kartläggning som nämndes inledningsvis i avsnitt 1.1. Maskininlärning är därför ett tveeggat svärd som kan användas både i skyddande och exploaterande syften.

2.5.3 Säkra flerpartsberäkningar

Säkra flerpartsberäkningar (*Secure Multi-Party Calculations* – MPC) är en gren inom kryptografin med målsättningen att låta flera aktörer samverka kring en algebraisk operation över respektive parts egna uppgifter, samtidigt som dessa hålls hemliga för övriga deltagande aktörer. Säkra flerpartsberäkningar kan utföras på ett flertal olika sätt, med olika styrkor och svagheter. Ett område relevant för säkra flerpartsberäkningar är homomorfisk kryptering. Denna teknik är ännu i sin linda och har i dagsläget begränsad användbarhet, men där betydande framsteg i utvecklingen mot praktiska tillämpningar gjorts de senaste åren.

Sådan kryptering har en formbarhetsegenskap som innebär att en operation på det krypterade datat är ekvivalent med samma operationen utförd på det avkrypterade datat. Homomorfisk kryptering bevarar således viss struktur i datat, så att analys och beräkningar kan göras över den krypterade informationen. Resultatet är emellertid inte användbart utan avkryptering.

Genom en fullständigt homomorfisk kryptering kan alltså en part kryptera de uppgifter som ska behandlas, varefter den andra parten sedan kan utföra godtyckliga behandlingar på de krypterade uppgifterna. Resultatet av behandlingen kan förmedlas tillbaka till den avsändande parten där de avkrypteras för att erhålla resultatet i klartext.

Det finns idag effektiva additiva och multiplikativa homomorfiska krypteringsmetoder, där de multiplikativa är begränsade till polynom av låg grad. Detta kallas delvis homomorfisk kryptering. För

att utföra godtyckliga algebraiska operationer över polynom av högre grad krävs emellertid användning av fullständigt homomorfisk kryptering vilket idag fortfarande är för beräkningsmässigt kostsamt för att ha praktisk tillämpning. Dock kan delvis homomorfisk kryptering utgöra lösningar på vissa specifika problem redan idag.

Nyttan med säkra flerpartsberäkningar inom området för skydd av den personliga integriteten, är att behandling av känsliga uppgifter i framtiden skulle kunna läggas ut på annan part, utan att dessa uppgifter röjs för den som utför behandlingen. Denna teknik skulle kunna användas främst inom två områden: dels vid samkörning av två eller flera register, där uppgifterna inte får röjas ens till den part som utför samkörningen; dels vid avidentifiering av uppgifter i register som ska användas vid analys för statistiska ändamål, där uppgifterna som avpersonifieras måste ingå som underlag för att producera meningsfulla resultat vid informationsutvinningen.

Det förstnämnda scenariet kan vara relevant till exempel om två eller flera vårdinrättningar behöver samköra register för att spåra tecken på epidemiska utbrott, om två myndigheter behöver jämföra registeruppgifter utan att dessa uppgifter överförs så att sekretessen bryts, eller om två underrättelseorganisationer behöver jämföra hemliga uppgifter. Det andra scenariet aktualiseras vanligen då olika känsliga register ska tillhandahållas för forskningsändamål. Statistisk analys skulle också kunna göras på flöden av e-post, för att med hjälp av Bayesiska filter som verkar över det krypterade datat sortera ut skräppost, utan att innehållet i den legitima e-posten riskerar att röjas till utomstående.

3 Inbyggt integritetsskydd

Inbyggt integritetsskydd (*"privacy-by-design"*) är ett term som används för att beskriva system och lösningar där skyddet för privatlivet är en integrerad del som tagits med som ett grundkrav från början vid utvecklingen av systemet eller lösningen, och som löper som en röd tråd genom systemets hela livscykel. Motsatsen till en sådan metodik är att försöka åstadkomma skydd i efterhand, då systemet eller lösningen är färdigutvecklad. Till exempel genom införande av informationssäkerhetsåtgärder som syftar till att förhindra att känsliga uppgifter röjs till obehöriga.

Det ska påpekas att termen *privacy-by-design* inte är helt entydig i dess tolkning. I dess ursprungliga definition utmejslas 7 grundregler[2], där flera delar känns igen och till stor del överlappar med dagens persondataskyddslagstiftning. Grundreglerna är i övrigt tämligen vaga och inte alldeles enkla att omsätta i praktiskt handlande. I denna skrift tas därför fasta på ett antal konkreta principer för inbyggt integritetsskydd:

Uppgiftsminimering – genom att systematiskt minimera mängden uppgifter som samlas in och behandlas förebyggs risker på ett proaktivt sätt;

Informerat medgivande – där användarvillkor presenteras på ett lättbegripligt, relevant och överskådligt sätt och ger användaren möjlighet att välja att inte dela vissa uppgifter;

Transparens – erbjuder användaren insyn i hur dennes uppgifter behandlas;

Förebyggande verifierbart skydd – risker förebyggs genom skyddsåtgärder vars effektivitet är verifierbara;

Möjlighet att återta ett medgivande – erbjuder användaren enkel möjlighet att ta tillbaka medgivande och att få relevanta uppgifter raderade.

Samtliga av dessa principer har sina motsvarigheter i personuppgiftslagen (1998:204); Uppgiftsminimering (9 § f), medgivande (10, 15 och 34 §§), transparens (26 §), skyddsåtgärder (31 §) och återtagande av medgivande (12 §) är delar i detta. Att tillämpa principerna för inbyggt integritetsskydd innebär emellertid att tillmäta dessa persondataskyddsaspekter central betydelse vid utformningen av ett system, och sedan föra med dessa tankebanor i varje fas i systemets livscykel. Men det innebär också att i många avseenden gå längre än den praxis som följer av lagstiftningen inom vart och ett av dessa områden, till exempel genom att tillämpa ett kritiskt tänkande och ifrågasättande av nödvändigheten med alla delar av behandlingen och att presentera användaren med relevanta valmöjligheter att avstå viss insamling och behandling.

Förekomsten av produkter och tjänster som genomgående konstrueras enligt dessa principer är förhållandevis sällsynta. Även om den teknik som behövs finns tillgänglig och är välbeprövad, kräver inbyggt integritetsskydd nya tankebanor.

Antag till exempel att en myndighet ska erbjuda medborgaren en e-tjänst där denna ska fylla i ett antal känsliga uppgifter, kanske för att erhålla en social förmån. Vid utformningen av e-tjänsten görs bedömningen att det är avgörande att den enskilde kan få hjälp på sådant sätt att vissa uppgifter kan inhämtas från en annan myndighet så att dessa blir förifyllda i formuläret.

Rent tekniskt är troligen det enklaste sättet att låta den första myndigheten få direktåtkomst till den andra myndighetens register via någon överföringsmekanism, vilket då skulle ske för ett angivet och berättigat ändamål. I detta uppstår emellertid betydande risker för den enskildes personliga integritet.

Intrång, säkerhetsöverträdelser eller misstag riskar medföra att uppgifter från båda registren röjs, överförs eller behandlas på ett sätt som inte varit avsett. I motsvarande grad uppstår även frågor om hur transparensen och efterlevnaden ska kunna säkerställas, så att det står helt klart att sådana säkerhetsöverträdelser inte skett eller sker. Slutligen är det juridiskt problematiskt att koppla samman myndigheters system på detta sätt. För att överföring ska komma till stånd

krävs stöd i någon sekretessbrytande bestämmelse. Offentlighets- och sekretesslagen (2009:400) innehåller heller ingen generell regel om överföring av sekretess när sekretessbelagda uppgifter överlämnas mellan olika myndigheter, vilket medför att en allmän handling som är skyddad genom sekretess vid den ena myndigheten inte med nödvändighet är skyddad då den överförts till en annan myndighet.

Ett sätt att minska riskerna, minimera mängden överskottsuppgifter, lägga grunden för ett informerat medgivande, skapa transparens, verifierbarhet och spårbarhet är att utforma tjänsten utifrån principerna för inbyggt integritetsskydd. I det här exemplet skulle de informationskällor som krävs för e-tjänsten kunna förses med programmatiska gränssnitt, där det är möjligt för den enskilde själv att med hjälp av sin e-legitimation begära ut de nödvändiga uppgifterna i maskinläsbart format direkt från respektive myndighet, för att sedan låta sammanställa dessa uppgifter i den egna omgivningen, till exempel i webbläsaren eller i en mobil applikation.

Detta förfarande skulle fungera ungefär som i den fysiska verkligheten, där den enskilde på egen hand begär ut sina egna uppgifter från varje myndighetsregister som är inblandat. Dessa uppgifter kan den enskilde sedan sammanställa, redigera och komplettera vid sitt eget köksbord, för att slutligen skriva under och skicka in handlingen till den mottagande myndigheten.

Genom att användaren i den elektroniska motsvarigheten själv, med hjälp av sin e-legitimation, direkt från respektive myndighet inhämtar de känsliga uppgifterna sker rent tekniskt aldrig någon direkt överföring myndigheterna mellan. E-tjänsten tillhandahåller det stöd som krävs för sammanställningen i användarens omgivning, där denne kan granska och komplettera de uppgifter som ska skickas in, *innan* de inkommer till den mottagande myndigheten.

Att direktåtkomst myndigheterna emellan undviks kan leda till att en annan juridisk bedömning kan göras när det kommer till de sekretessrelaterade frågorna, och frågorna kring när en handling kan anses vara inkommen till den mottagande myndigheten.

Ett sådan teknisk lösning är inte särskilt komplicerad, men fordrar att myndighetens jurister, systemutvecklare och verksamhetsutvecklare alla samverkar kring målet att minimera de risker som sammanlänkning av känsliga register annars medför. Grundläggande blir således även att förstå riskerna, på vilket sätt de kan undvikas och i varje steg tillämpa ett kritiskt tänkande och ifrågasättande av hur

personuppgifter måste hanteras.

3.1 Uppgiftsminimering

Uppgiftsminimering är ett av de absolut mest effektiva sätten att lindra risker gällande den personliga integriteten. Generellt ska enbart uppgifter samlas in som är nödvändiga för ändamålet, och sparas endast så länge som de behövs. Effektiv uppgiftsminimering kan emellertid innebära att gå längre än så, till exempel genom att avpersonifiera vissa poster, undvika att använda direkta identifierare eller konsolidera vissa uppgifter för att göra dem mindre känsliga.

Till exempel skulle en vädertjänst, som via en mobil applikation levererar prognos för den plats där användaren befinner sig, i syfte att tillhandhålla denna tjänst regelbundet kunna samla in uppgifter om användarnas positioner. Utan att tillämpa långgående principer för uppgiftsminimering finns stor risk att det uppstår en koncentrerad informationskälla hos leverantören av vädertjänsten, innehållande betydande mängder känsliga personuppgifter.

Även om den mobila enhetens GPS tillhandahåller position med ett par meters noggrannhet, kan det förmodas att prognosen gäller för ett betydligt större område. De positionsangivelser som skickas till bakomliggande system skulle därför kunna påföras brus eller avrundas till några kilometers radie. Samtidigt kanske det inte är nödvändigt att alltid, varje gång applikationen startar, inhämta position. Många gånger kan det förväntas att användaren endast vill se väderprognosen kring hemmet och andra favoritplatser - och inte där man för närvarande råkar befinna sig. En enkel knapp i applikationen för att uppdatera till aktuell position kan förväntas reducera mängden inkomna positionsangivelser påtagligt.

Ett annat sätt att minimera mängden uppgifter som måste inhämtas kan vara att endast spara användarens favoritplatser i applikationen i den mobila enheten, och inte i det bakomliggande systemet. På så sätt undviks att det uppstår ett centralt register med denna information om alla tjänstens användare, vilket kan förväntas lindra riskerna ytterligare. Logginformation som relaterar till användare, och som unikt identifierar en användare bland andra (t.ex. den mobila enhetens pseudonyma identitet) bör kunna gallras eller avidentifieras tämligen omgående i en sådan här situation. Det är svårt att se att det krävs att logginformation sparas någon längre tid för att tillgodose

nödvändiga behov av spårbarhet.

Uppgiftsminimering kan även innefatta att försöka undvika att behandla direkta identifierare, till exempel namn eller personnummer. I detta kan användning av biometriska avtryck, till exempel ett fotografi eller ett fingeravtryck, i vissa tillämpningar fungera som uppgiftsminimerande och integritetsskyddande teknik. Sådana biometriska avtryck är betydligt svårare att korrelera och samköra jämfört med andra direkta identifierare som namn, personnummer och adress. Ett exempel utgör kollektivtrafikbiljetter som i vissa fall av affärsmässiga skäl måste vara personliga, vilket många gånger fordrar att resenären ska kunna legitimera sig med fullgod fotolegitimation. Ett alternativ till att registrera biljetten med namn och kundnummer kunde vara att erbjuda resenären att istället knyta biljetten till ett fotografi (en *"selfie"*). Om fotografiet kan lagras på ett säkert sätt på biljettmediat behöver inga personuppgifter behandlas i de centrala systemen. Ytterligare fördelar nås genom att personer som inte innehar fotolegitimation (minderåriga, med flera) kan åka med kollektivtrafiken. Riskerna minskar och möjligheterna ökar.

3.2 Informerat medgivande

För behandling av personuppgifter krävs enligt personuppgiftslagen att den personuppgifterna rör ska samtycka till behandlingen. För att samtycket ska vara giltigt ska den registrerade ha fått tillräcklig information om behandlingen. Den registrerade måste ha fått sådan information att han eller hon kan ta ställning till om hans eller hennes personuppgifter ska få behandlas för det ändamål och på det sätt som planerats.

I praktiken är det dock många gånger svårt att nå användarförståelse och faktiskt informerat medgivande. Ofta är rutinerna för att tillhandahålla informationen i första hand utformade utifrån leverantörens behov, snarare än att användaren ska kunna ta ett informerat beslut.

Figur 3.1 visar en typisk användardialog i en tvåpartsrelation som till exempel förekommer när en ny mobil enhet för första gången ska tas i bruk av konsumenten. Då måste leverantörens användarvillkor (inklusive villkor för behandling av personuppgifter) godkännas.

Information om personuppgiftsbehandlingen är ofta inbakade i obegripliga och närmast ändlösa slutanvändaravtal som med varje

rimlig ansträngning är fullkomligt ogenomträngliga, och som knappast utgör den typen av litteratur som en användare ämnar spendera timmar att fördjupa sig i. Användaren ges heller inga alternativ kring vilka uppgifter som ska delas med vem och hur. Vill konsumenten använda den produkt denne köpt finns bara alternativet att godkänna villkoren.

För den som till äventyrs ändå läser slutanvändaravtalet framgår att tillverkaren framställer en unik identifierare kopplad till enheten och därmed innehavaren, som används för att kartlägga användarens positioner, vanor och intressen genom dennes användning av enheten, för att sedan kunna rikta reklam till användare. Funktionen är påslagen utan att användaren gjort några val eller på något annat relevant sätt informerats om den. Att funktionen existerar framgår i praktiken först när användaren letat sig längst ner i en undermeny under integritetsskydd i enhetens inställningar. Där finns ett otydligt val att begränsa spårning och att återställa den unikt framställda identifieraren. Det går inte att välja bort att delta annonsprogrammet, och det går heller inte att ställa in enheten att regelbundet med något intervall låta återställa identifieraren.

Figur 3.1 – Dialogruta utformad utifrån leverantörens behov.

Användardialogen i figur 3.2 är däremot utformad utifrån konsumentens behov, och skulle kunna förekomma då användaren installerar en tredjepartsapplikation i tidigare nämnda mobila enhet. Dessa applikationer installeras i egna fack i den mobila enhetens operativsystem, och måste begära och beviljas åtkomst till andra funktioner utanför det egna facket, till exempel kontaktbok, bilder, lokaliseringsinformation, med mera. Genom användardialogen erbjuds konsumenten möjligheten att använda applikationen även utan att dessa uppgifter delas med applikationen, och med det även leverantören

av applikationen. Det finns menyval för att senare kontrollera vilka applikationer som givits åtkomst till vad, och dessa inställningar kan enkelt ändras.

Dialogrutan är också utformad för att vara felsäker på ett sådant sätt att förvalet, och det val som står först, är att inte tillåta någon åtkomst. För användare som inte förstår eller missar i dialogen blir resultatet minsta möjliga behandling av personuppgifter, det vill säga *opt-in* i övriga delar.

Figur 3.2 – Dialogruta utformad utifrån användarens behov.

Sammantaget kan sägas att leverantören i det här exemplet väl omhändertar användarens intressen gentemot tredjepartsleverantörer av applikationer, men agerar på ett helt annat sätt i den egna relationen mot användaren.

3.3 Transparens

Att erbjuda transparens innebär att låta användaren själv få insyn i vilka uppgifter som behandlas och på vilket sätt, till exempel genom att visa hur uppgifter kan komma att överföras till andra aktörer (och koppla detta till informerade val, enligt 3.2).

En annan viktig del i transparensen är att tjänstetillhandahållaren åtar sig att informera användaren vid förekomst av intrång eller säkerhetsöverträdelser som kan ha lett till att dennes personuppgifter har röjts till obehöriga. Tjänstetillhandahållaren bör ha inrättat processer och rutiner för hur användare ska underrättas vid en sådan händelse.

3.4 Förebyggande verifierbart skydd

Det är många gånger svårt att avgöra verkan av införda informationssäkerhetskontroller. Möjligen kan kontrollernas effektivitet mätas gentemot funna avvikelser eller inträffade incidenter, men inom en tjänst eller i ett system med betydande risker för de enskildas personliga integritet är det knappast godtagbart att pröva sig fram i denna del.

Verifierbart skydd grundas ofta i olika former av kryptering där nyckelmaterial hanteras i särskild manipulationsskyddad hårdvara. Hårdvaran ska skydda nycklarna från att röjas och medger trovärdig spårbarhet vid användning av dem. Skyddet kan till exempel användas för att lagra information krypterat då den inte används, eller för att åstadkomma separation av arbetsuppgifter.

Skyddet för informationen kan också upprätthållas med hjälp av genomgående kryptering, innebärande att användarens uppgifter är krypterade med nyckelmaterial som endast användaren (fysiskt och logiskt) förfogar över. Ett exempel kan vara en säkerhetskopia av känslig karaktär som är krypterad med ett tillräckligt komplicerat lösenord som endast användaren känner till. Säkerhetskopian skulle därvid kunna förvaras hur som helst, så länge dess tillgänglighet är säkerställd. Oavsett är skyddet verifierbart på det sätt att informationen inte kan röjas till obehöriga så länge lösenordet endast är känt för den som äger informationen.

Ofta krävs dock mer avancerade krypteringsfunktioner för att åstadkomma användbara tjänster, till exempel asymmetrisk kryptografi. Med asymmetriska algoritmer avses sådana kryptografiska funktioner där ett nyckelpar används, bestående i en publik komponent och en privat komponent, som står i sådant motsatsförhållande till varandra att det som krypteras med den ena komponenten kan avkrypteras med den andra, och vice versa.

Genom att använda asymmetrisk kryptografi kan en part skicka ett meddelande som endast kan avkrypteras av mottagaren, förutsatt att den avsändande parten har tillgång till den mottagande partens publika nyckel. Ett problem för att på ett bra sätt använda sådan kryptering för innehåll i webbtjänster har varit att det saknats gränssnitt för nyckelhantering och krypteringsfunktioner i de vanligt förekommande webbläsarna. Det pågår dock viktigt och långt framskridet standardiseringsarbete på detta område, där de flesta webbläsare

redan idag också har stöd för utkastversionerna av denna standard framtagen inom W3C och kallad *Web Cryptography API*.

Ett användningsområde för sådan genomgående kryptering skulle kunna vara en meddelandetjänst, med vilken myndigheter kan förmedla krypterad elektronisk post innehållande uppgifter som annars skulle kräva att de skickades med traditionellt brev. Användare skulle med hjälp av e-legitimation kunna registrera sina publika nycklar, som myndigheten sedan kan använda för att kryptera meddelandena med. När meddelandet är skyddat kan det förmedlas via vilka kanaler som helst, och den operatör som tillhandahåller det elektroniska brevlådeutrymmet till användaren kan aldrig ta del av innehållet. På detta sätt erhålls ett verifierbart starkt skydd för uppgifterna.

På detta sätt är skyddet för uppgifterna inte beroende av den kedja av kontroller som annars skulle behöva sättas på plats vid en sådan brevlådeoperatör, innefattande fysisk och logisk åtkomstkontroll, behörighetsstyrning, stark autentisering, personalsäkerhet, säker hantering av lagringsmedia, loggning och logguppföljning, styrmedel för elektronisk kommunikation, et cetera. En kedja som är mycket svår och även kostsam att låta verifiera, och erbjuder endast begränsad transparens – även med sådan verifiering utförd av tredje part. En systemtekniker behöver i sitt arbete ofta åtkomst på operativsystemnivå, och har där som regel möjlighet att åsidosätta alla andra åtkomstkontroller[1]. Med genomgående kryptering på plats kan emellertid en brevlådeoperatör inte röja uppgifterna.

3.5 Möjlighet att återta ett medgivande

För att kunna tillvarata den enskildes rätt att ta tillbaka ett medgivande att behandla dennes personuppgifter på ett relevant sätt, måste ett system vara konstruerat med denna funktion i åtanke från början. Modern systemdrift sker idag i distribuerade *servermoln* där lagring av uppgifterna är likaledes distribuerade. Uppgifter existerar även i generationer av säkerhetskopior, varav vissa kanske förvaras från-

[1] Jmf. hur Edward Snowden som arbetade som systemadministratör vid NSA kunde röja stora mängder hemligstämplade uppgifter utan upptäckt.

kopplat på geografiskt skilda platser. Det är således inte praktiskt genomförbart att säkert radera varje förekomst av dessa uppgifter. Lösningen kan istället vara att varje post som relaterar till en användare krypteras med en för användaren specifik krypteringsnyckel. Vid händelse att användaren begär att få sina uppgifter raderade utplånas denna krypteringsnyckel, varvid alla uppgifter som relaterar till användaren blir oläsliga.

Det finns förstås samtidigt uppgifter som måste sparas även efter att en användare återtagit ett medgivande, och som kan relatera till användaren och dennes användande av en tjänst i olika grad. Exempel innefattar ekonomiska underlag, viss logginformation, et cetera.

4 Ett ledningssystem för persondataskydd

Som framgått av föregående avsnitt är det skillnad på att som organisation efterleva gällande persondataskyddslagstiftning och att tillämpa principerna för inbyggt integritetsskydd. Även om inbyggt integritetsskydd på ett effektivt sätt lindrar riskerna i behandlingen av personuppgifter kan det också förväntas driva kostnader. Vidare krävs särskild specialistkompetens för att avgöra på vilket sätt principerna för inbyggt integritetsskydd kan omsättas i risklindrande åtgärder, till exempel på vilket sätt integritetsskyddande teknik kan nyttjas och integreras. Samtidigt är det vanligen externa intressenters krav som utgör drivkraften bakom persondataskyddet, där arbetet med persondataskyddet till sist är en förtroendefråga. Det gör det svårt att inom ett utvecklings- eller införandeprojekt prioritera dessa krav i förhållande till andra möjligen mer handfasta krav som till exempel leveranstidpunkter och kostnadsramar.

Det innebär att tillämpningen av principerna för inbyggt integritetsskydd snarare är en ledningsfråga än en fråga som kan drivas inom verksamheten eller i ett projekt. Ledningen bör ha visat åtagande i fråga om tillämpningen av principerna, genom att fastställa mål med persondataskyddsarbetet och hur ansvaret för att nå uppsatta mål är fördelat. Det behöver även finnas den kompetens tillsatt som krävs och tillräckliga medel för att driva och samordna arbetet med persondataskyddet.

Att på detta sätt tillvarata olika intressenters krav och förväntningar på en organisation har sina tydliga paralleller inom flera andra områden, till exempel miljöskydd, informationssäkerhet och kvalitet. Inom vart och ett av dessa områden finns internationella etablerade ledningssystemstandarder. Mot respektive standard kan en organisation låta certifiera sitt ledningssystem, för att på så sätt visa gentemot

intressenterna att organisationen arbetar målinriktat med dessa frågor enligt vissa vedertagna normer och principer.

Ett intressant utvecklingsområde kunde därför vara att undersöka möjligheten att ta fram en standard för ledningssystem för persondataskydd, som i sin tur inbegriper principerna för inbyggt integritetsskydd. Efterlevnad av en sådan standard skulle, på samma sätt som inom de andra områdena, kunna bli en kvalitetsmärkning kring vilken det skapas en kommersiell efterfrågan. Det skulle också vara ett medel för att genom systematik integrera persondataskyddsfrågorna i verksamheten, skapa delaktighet bland medarbetarna, samt stärka varumärket och öka förtroendet för en organisation som fäster vikt vid att värna om den personliga integriteten.

5 Referenser

[1] M. Barbaro and T. Jr. Zeller, *A face is exposed for AOL searcher no. 4417749*, The New York Times (2006).

[2] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, (2009), Revised: January 2011.

[3] D. Chaum, A. Fiat, and M. Naor, *Untraceable electronic cash*, Proceedings on Advances in Cryptology, CRYPTO '88, Springer-Verlag New York, Inc., 1990, pp. 319–327.

[4] IIS (Stiftelsen för internetinfrastruktur), EY, Bankgirot och Swedbank, *Sverige betalar*, Insight intelligence, september 2015.

[5] Arvind Narayanan and Vitaly Shmatikov, *Robust de-anonymization of large sparse datasets*, Proceedings of the 2008 IEEE Symposium on Security and Privacy (Washington, DC, USA), SP '08, IEEE Computer Society, 2008, pp. 111–125.

Rapport från Rättssociologiska institutionen och Lunds universitets internetinstitut 2016

Digitalisering och personlig integritet

Digitalisering och personlig integritet

En systematisk kunskapsöverikt

Framtagen av Lunds universitet i samarbete mellan Lunds universitets internetinstitut, Rättssociologiska institutionen och Universitetsbiblioteket

Projektledare

Måns Svensson, docent i rättssociologi

Författare

Calle Rosengren
Måns Svensson
Fredrik Åström

Innehållsförteckning

Innehållsförteckning 4
Sammanfattning 5
1. Inledning 6
2. Metod 7
(a) Planering av studien 7
(b) Söka, identifiera och organisera artiklar 7
(c) Extrahera och värdera materialet 8
3. Resultat 9
Bibliometrisk analys 9
Systematisk litteraturöversikt 20
Teknik 24
Lagstiftning 28
Stat 32
Generella teoretiska resonemang 37
Arbete 40
Kunskap och beteende bland unga 43
Hälsa 46
Handel 49
Privata relationer 52
Mänskliga rättigheter i det digitala 54
Sousveillance 56
Övrigt 57
Beteende 58
4. Artiklar vilka byger på empiriska studier indelade utifrån metod 59

Sammanfattning

Forskningsområdet *digitalisering och personlig integritet*, så som det definierats och avgränsats (framförallt genom val av söksträngar), inom ramen för den här kunskapsöversikten, är under tillväxt. Föreliggande studie har begränsats till engelskspråkiga artiklar publicerade i vetenskapliga peer-review-granskade tidsskrifter. Under de senaste 10 åren har antalet vetenskapliga artiklar per år inom området mer än femdubblats. Exempelvis ger en sökning i forskningsdatabasen WEB OF SCIENCE avseende 2006 13 träffar medan en identisk sökning avseende 2014 ger 72 träffar.

I den här systematiska kunskapsöversikten har två typer av undersökningar genomförts. För det första en bibliometrisk analys som syftar till att, på en statistisk analytisk nivå, skapa en övergripande bild av hur forskningen på området ser ut. För det andra en systematisk litteraturstudie där relevanta vetenskapliga artiklar har identiferats, analyserats innehållsmässigt och kategoriserats.

Den bibliometriska analysen visar att det föreligger en tämligen strikt uppdelning av forskningen om digitalisering och personlig integritet mellan huvudsakligen tre vetenskapliga fält. Det vill säga att kommunikationen mellan fälten (i termer av att referera och citera varandras arbeten) är förhållandevis begränsad. Forskningsfälten kan beskrivas som (a) ett tekniskt fält som i hög grad handlar om systemutveckling, (b) ett juridiskt fält med fokus på frågor om lagstiftat skydd av personlig integritet, samt (c) ett mer samhälls- och beteendevetenskapligt orienterat fält som bland annat samlar informatik, psykologi, sociologi, statsvetenskap och marketing- och managementforskning.

Den systematiska litteraturöversikten, som baseras på en genomläsning av samtliga ingående artiklar, visade att det även inom de olika vetenskapliga disciplinerna saknas tydliga gemensamma begreppsapparater och gemensam syn på metod. Dock kan man se ett antal olika områden (eller forskningsfokus) vilka är frekvent återkommande. De fem dominerande områdena är: (a) teknik, (b) lagstiftning, (c) stat, (d) teori och (e) arbetsliv.

Dessutom kan man i forskningen identifiera olika förhållningssätt i förhållande till digitalisering och personlig integritet. För det första *som ett problem* (eller kanske snarare utmaning) som går att hantera med hjälp av ny, bättre och mer integritetskänslig teknik. För det andra *som en möjlighet* att genom nyttiggörandet av potentiellt integritetskänslig data kunna verka för goda värden såsom förbättrad hälsa. För det tredje *som ett hot* mot medborgare och anställda. Och till sist som *en utbytesrelation* mellan nytta och risk, exempelvis avseende staters behov av information för att förebygga hot och medborgares rätt till integritet.

Slående är att det saknas tillräcklig kunskap avseende relationen mellan övervakning i det digitala och eventuella beteendeförändringar i samhället. Olika studier pekar på risker för att bristande respekt för den privata integriteten kan leda till minskat internetanvändande och minskat politiskt engagemang (åtminstonde på nätet). Dock saknas det ännu empiriska bevis för att så skulle vara fallet.

1. Inledning

Föreliggande kunskapsöverikt har genomförts av Lunds universitet på uppdrag (reglerat i avtal 2015-04-23) av Integritetskommittén (Ju 2014:09). Integritetskommitténs arbete preciseras genom direktiv 2014:65 som anger att den parlamentariskt sammansatta kommittén skall: Utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet samt inom ramen för detta arbete följa upp effekterna i lagstiftningsarbetet av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes 2011, och med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av kartläggnings- och analysuppdraget, följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd och särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet, samt föreslå nöd- vändiga författningsändringar.

Det uppdrag från Integritetskommittén som ligger till grund för den här kunskapsöversikten har formulerats enligt följande: I kunskapsöversikten skall framgå vilka studier av intresse som har gjorts både här i Sverige och i omvärlden när det gäller frågan om hur individer, grupper och samhällen påverkas av att vara övervakade, tro sig vara övervakade, eller av att de kan bli föremål för övervakning (även om de inte blir det). Detsamma gäller studier om hur människor, inklusive organisationer och företag, har påverkats av de möjligheter som nu finns att aktivt övervaka/kontrollera andra. Med påverkan avses hur inställning/synsätt och beteende förändras. Av kunskapsöversikten skall vidare framgå om studier har gjorts inom särskilda områden, exempelvis om patienters inställning och hur de påverkas, eller om arbetsgivares beteende påverkats, både i samband med nyrekrytering och beträffande sina anställda. Om eventuella skillnader i synsätt och beteende mellan olika kön har behandlats i någon studie skall det lyftas fram, liksom skillnader mellan olika åldrar. Det är t.ex. av intresse om det finns studier gällande barn som växer upp i den digitala miljön.

Metoden som använts för uppdraget är den vetenskapliga systematiska litteraturstudien samt bibliografisk analys. Sökningar på svenska gav ytterst få träffar, varför den delen av uppdraget lämnas därhän. Fokus ligger på vetenskapliga peer-review-granskade artiklar på engelska.

2. Metod

I grunden är den systematiska kunskapsöversikten en forskningsstudie som samlar in, analyserar och sammanställer studier inom ett visst område (eller utifrån en specifik frågeställning). Således kan den systematiska kunskapsöversikten beskrivas som ett sätt att sammanställa kunskapsläget inom ett visst område genom en strukturerad och systematisk insamling och granskning av vetenskapliga studier. Insamlingen av olika studier sker oftast genom sökning efter vetenskapliga publikationer i databaser (t ex EBSCO eller Web of Science) och styrs då av relevanta sökord. Genom att metod, utgångspunkter och sökkriterier synliggörs säkras transparens och möjligheten att replikera studien ökar. Inom ramen för föreliggande kunskapsöversikt används de tre steg som Tranfield et al. (2003) beskriver i *Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review* (2003): (a) Planering; (b) söka, identifiera och organisera publikationer; samt (c) extrahera och värdera. Vid varje steg krävs det ett antal överväganden vad gäller såväl sökkriterier som frågor rörande vilka publikationer som ska inkluderas respektive exkluderas. Nedan redovisas hur Transfields (et al.) metod har applicerats inom ramen för föreliggande studie.

(a) Planering av studien

Kunskapsöversikten fokuserar frågor som rör digitalisering och personlig integritet. Av särskilt intresse är övervakning genom det digitala mediet samt dess eventuella konsekvenser för attityder, beteende och integritet/privatliv. Om möjligt skall studien kunna belysa specifika gruppers förutsättninar (exempelvis baserat på ålder och kön), samt identifiera tematiska områden för vilka frågeställningen är relevant.

Viktiga avgränsningar utgörs av det faktum att det systematiska sökandet efter vetenskapliga publikationer i den här studien begränsas till artiklar i vetenskapliga tidsskrifter vilka är skrivna på engelska. De publikationer inom området som finns på svenska är i regel inte vetenskapliga i den meningen att de inte är peer-review-granskade och därmed inte har genomgått den process som garanterar vetenskaplig kvalitet. Det här gäller i synnerhet för artiklar, men i hög utsträckning även för böcker och rapporter. Ett viktigt undantag utgörs av doktorsavhandlingar vilka uppfyller vetenskapliga krav, men som ändå faller utanför begränsningarna för den här studien. Med detta sagt är det viktigt att understryka att relevant kunskap om specifka svenska förhållanden kan återfinnas i så kallad grålitteratur (ej vetenskapligt granskade rapporter, myndighetstryck, fackböcker etc.) som inte redovisas här.

(b) Söka, identifiera och organisera artiklar

Digitaliseringen av samhället har utifrån ett integritetsperspektiv inneburit stora utmaningar som rör ett flertal olika forskningsfält. De frågor som hanteras rör relationer mellan stat och medborgare, mellan konsument och företag, mellan arbetsgivare och arbetstagare och även mellan enskilda individier. Tekniken erbjuder nya möjligheter att kommunicera och serva kunder och medborgare, men samtidigt oanade möjligheter att kartlägga individers åsikter och beteende. Ambitionenen med denna kunskapsöversikt är att skapa en så bred bild som

möjligt av var forskningen avseende digitalisering, integritet och påverkan på människor står.

För denna systematiska kunskapsöversikt bedömdes att det framförallt var två databaser som var lämpliga och det är SCOPUS samt Web of Science (Core collection). SCOPUS, som ägs av Elsevier, indexeras ca 22 000 vetenskapliga tidskrifter och har en bred täckning vad gäller olika discipliner och ämnen. Web of Science är en databas (inkluderande bland annat 12 000 vetenskapliga tidskrifter av högsta kvalitet) publicerad av Thompson Reuters som förtecknar internationell forskningslitteratur, framför allt tidsskriftsartiklar på engelska. Fördelen med denna databas är att informationen är innehållsmässigt rik och möjliggör långtgående bibliometriska analyser.

(c) Extrahera och värdera materialet

I syfte att ge en så heltäckande bild som möjligt över kunskapsläget har vi för denna systematiska kunskapsöversikt valt att genomföra såväl en bibliometrisk analys som en systematisk litteraturöversikt. En bibliometrisk analys handlar i grunden om att, med hjälp av statistiska analyser av texters och textsamlingars egenskaper, skapa en bild av inom villka forskningsfält som en företeelse (eller fenomen) studeras samt i vilken utsträckning som dessa fält relaterar sina resultat till andra fälts studier av samma företeelse. En systematisk litteraturöversikt är i princip en sammanställning av relevant litteratur inom ett specifikt område. Insamligen bygger på en noggrann och systematisk metod för litteratursökning. Till skillnad från, och som komplement till den bibliometriska analysen, innehåller denna metod även en kvalitativ komponent i det att litteraturen som söks ut även läses och värderas.

3. Resultat

Bibliometrisk analys

För att ge en överblick över vilka forskningsfält som behandlar frågor om personlig integritet i digitala sammanhang, samt vilka frågor denna forskning behandlar, genomfördes bibliometriska analyser av forskningslitteraturen.

De bibliometriska analyserna är baserade på sökningar i Web of Science-databaserna (WoS), en samling databaser som framför allt indexerar artiklar på engelska publicerade i internationella vetenskapliga tidskrifter. Nackdelen med att använda dessa databaser är att den forskningslitteratur som publiceras på andra språk och/eller i andra dokumenttyper (t.ex. böcker) inte blir tillgänglig. Fördelen är att WoS, förutom vanliga former av metadata som t.ex. författare och titel, också indexerar referenserna i de vetenskapliga texterna, vilket gör det möjligt att göra olika typer av citerings- och begreppsanalyser.

För att identifiera den forskningslitteratur i WoS som behandlar frågor om personlig integritet och övervakning i digitala sammanhang användes följande söksträng i ”topic”-fältet (som täcker begrepp som förekommer i titel, abstrakt och nyckelord): (Surveill*) AND (online* OR digital* OR Internet*) AND (behav* OR attitud* OR privac* OR "norms"). Vidare begränsades sökningen dels i tid, till perioden 2005-2015, dels ifråga om dokumenttyp, där endast original- och översiktsartiklar inkluderades i sökningen (Figur 1).

> You searched for: TOPIC: ((Surveill*) AND (online* OR digital* OR Internet*) AND (behav* OR attitud* OR privac* OR "norms"))
> Refined by: DOCUMENT TYPES: (ARTICLE OR REVIEW)
> Timespan: 2005-2015.
> Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.
> Results: 506

Figur 1. Söksträng för den Web of Science-sökning som bildar bas för datainsamling för de bibliometriska analyserna.

Sökningen resulterade i 506 artiklar, men i och med att begrepp som t.ex. ”surveillance”, även när de kopplas till begrepp som hanterar digitala sammanhang eller frågor om beteende, fångar in vetenskapliga artiklar som inte är relevanta för det sammanhang som analyseras här. Exempel på detta är ”surveillance” som ett viktigt begrepp inom epidemiologin, bevakning av patienter i samband med operationer eller hälso- och riskbeteenden vid t.ex. vård av missbrukare. Det rör sig alltså mer om övervakning som en vårdmetod snarare än säkerhets- och integritetsfrågor i samband med hantering av patientinformation. För att i så stor utsträckning undvika irrelevant litteratur gjordes ytterligare en begränsning där ett 50-tal WoS-kategorier (kategorier som beskriver tidskrifters huvudsakliga ämnesinnehåll) exkluderades ur

sökningen, vilket resulterade i en ny uppsättning omfattande 311 artiklar (Figur 2).

Refined by: [excluding] WEB OF SCIENCE CATEGORIES: (RESPIRATORY SYSTEM OR INFECTIOUS DISEASES OR RADIOLOGY NUCLEAR MEDICINE MEDICAL IMAGING OR PHARMACOLOGY PHARMACY OR ECOLOGY OR PERIPHERAL VASCULAR DISEASE OR SOCIAL SCIENCES BIOMEDICAL OR TROPICAL MEDICINE OR PARASITOLOGY OR MEDICINE GENERAL INTERNAL OR PSYCHOLOGY CLINICAL OR GENETICS HEREDITY OR ENDOCRINOLOGY METABOLISM OR FOOD SCIENCE TECHNOLOGY OR DERMATOLOGY OR ONCOLOGY OR VETERINARY SCIENCES OR IMMUNOLOGY OR TOXICOLOGY OR ENGINEERING BIOMEDICAL OR SURGERY OR CLINICAL NEUROLOGY OR PEDIATRICS OR BIODIVERSITY CONSERVATION OR PATHOLOGY OR BIOCHEMISTRY MOLECULAR BIOLOGY OR SUBSTANCE ABUSE OR OBSTETRICS GYNECOLOGY OR MEDICINE RESEARCH EXPERIMENTAL OR AGRICULTURE MULTIDISCIPLINARY OR ERGONOMICS OR REHABILITATION OR ZOOLOGY OR VIROLOGY OR GASTROENTEROLOGY HEPATOLOGY OR UROLOGY NEPHROLOGY OR OPHTHALMOLOGY OR OCEANOGRAPHY OR NUCLEAR SCIENCE TECHNOLOGY OR METEOROLOGY ATMOSPHERIC SCIENCES OR ENVIRONMENTAL SCIENCES OR MARINE FRESHWATER BIOLOGY OR LIMNOLOGY OR MATHEMATICAL COMPUTATIONAL BIOLOGY OR FISHERIES OR ENTOMOLOGY OR EMERGENCY MEDICINE OR ELECTROCHEMISTRY OR CHEMISTRY ANALYTICAL OR CARDIAC CARDIOVASCULAR SYSTEMS OR BIOCHEMICAL RESEARCH METHODS)
Results: 311

Figur 2. Forskningsfält exkluderade ur Web of Science-sökningen.

Avgränsningen resulterade i en mer begränsad dokumentmängd med färre irrelevanta dokument. Men ser man till de enskilda artiklar som fångas in (exemplifierat nedan av de tio senast indexerade dokumenten funna i sökningen), kan man se att det fortfarande finns artiklar som ligger vid sidan om fokus för denna litteraturöversikt. Att göra ytterligare avgränsningar i sökningen i WoS är svårt eftersom man då riskerar att exkludera allt för mycket litteratur som skulle kunna vara relevant.

Brown, S. 2015) Moving elite athletes forward: examining the status of secondary school elite athlete programmes and available post-school options. Phys Ed Sport Ped, 20(4), 442-458.
Hall, EC. & Willett, RM. (2015). Online Convex Optimization in Dynamic Environments. IEEE J Select Topics Signal Proc, 9(4), 647-662.
Ramsey, LR. & Hoyt, T. (2015). The Object of Desire: How Being Objectified Creates Sexual Pressure for Women in Heterosexual Relationships. Psych Women Quart, 39(2), 151-170.
Park, MS. Et.al. (2015). Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. Psych & Marketing, 32(6), 601-610.
El Maadi, A. & Djouadi, MS. (2015). Using a Light DBSCAN Algorithm for Visual Surveillance of Crowded Traffic Scenes. IETE J Res, 61(39, 308-320.
Lukacs, V & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. Inform Commun & Soc, 18(5), 492-508.
Cover, AY. (2015). Corporate Avatars and the Erosion of the Populist Fourth Amendment. Iowa Law Rev, 100(4), 1441-1502.

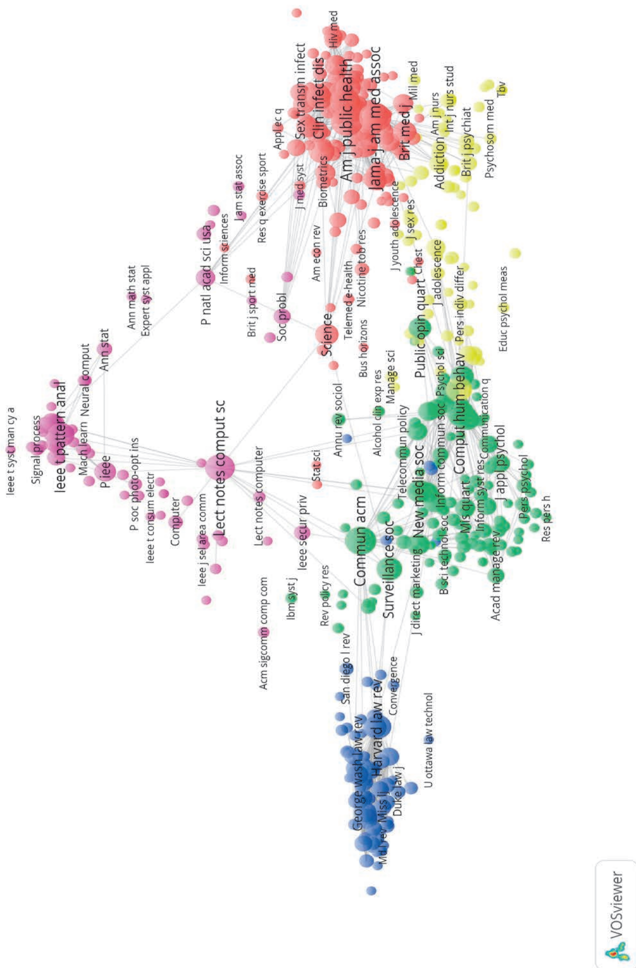
Roberts, A. (2015). Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. Mod Law Rev, 78(3), 535-548.
Cavazos-Rehg, PA. Et al. (2015). Monitoring of non-cigarette tobacco use using Google Trends. Tobacco Control, 24(3), 249-255.
Lee, HK. & Choo, HJ. (2015). Daily outfit satisfaction: the effects of self and others' evaluation on satisfaction with what I wear today. Int J Consum Stud, 39(3), 261-268.

Figur 3. Exempel på heterogenitet i artiklar funna i Web of Science-sökningen. De tio senast indexerade artiklar i dokumentsetet.

Informationen från WoS om de återstående 311 artiklarna laddades ner. För att bearbeta data användes Bibexcel (https://bibliometrie.univie.ac.at/bibexcel/), ett program för bibliometriska analyser där man bl.a. kan renodla informationen från WoS för att analysera specifika fält, t.ex. titel, författare eller citerade referenser; men också delar av specifika fält, t.ex. tidskriftsnamnen för citerade referenser. De data som framtagits genom Bibexcel användes sedan vidare i VOSviewer, version 1.6, (http://www.vosviewer.com/), ett program för utförande och visualisering av bibliometriska nätverksanalyser.

Analys av forskningsfält
För att identifiera vilka forskningsfält som studerar frågor om övervakning och personlig integritet valdes co-citeringsanalys på tidskriftsnivå. Tanken är att man studerar den litteratur som forskningen använt genom att analysera referenslistorna och antar att artiklar eller – i detta fall – tidskrifter som citeras tillsammans har ett ämnesmässigt samband. Om man gör dessa analyser baserat på hundratals eller tusentals artiklar med 10 000- eller 100 000-tals referenser, så bildar samförekommande citerade artiklar eller tidskrifter kluster som representerar olika forskningsinriktningar eller forskningsfält.

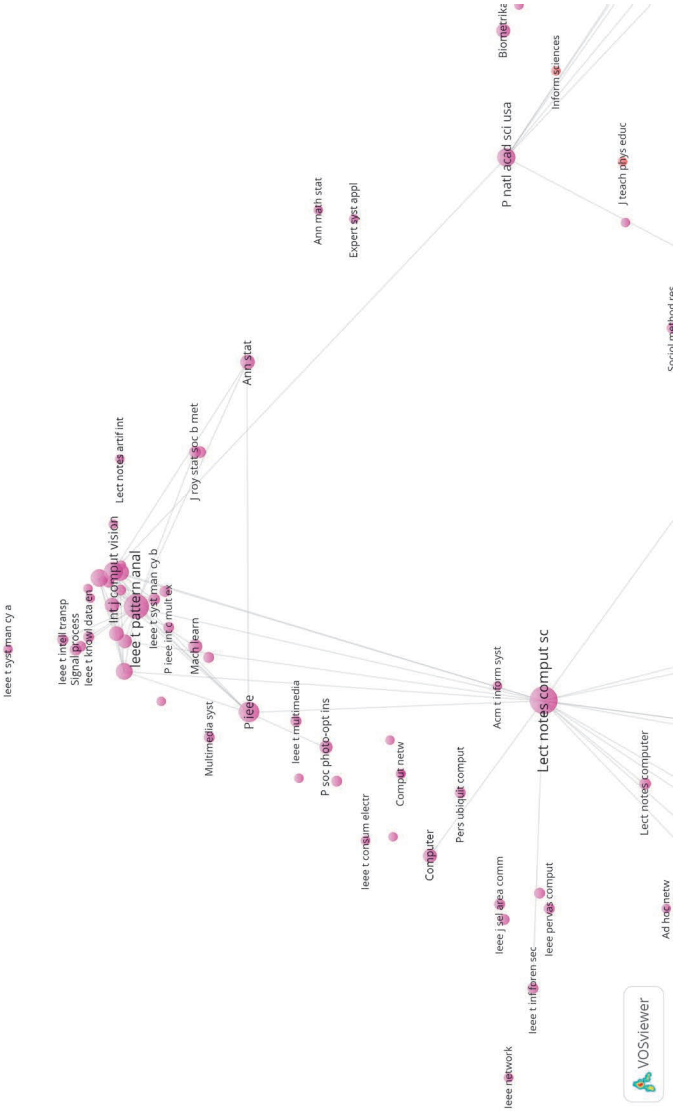
Följande analys bygger alltså på hur ofta citerade tidskrifter förekommer tillsammans i referenslistorna för de artiklar som identifierades i sökningen efter litteratur om integritet och digital övervakning. Kartan är baserad på analyser av de 500 mest citerade tidskrifterna. På kartan ser vi dels vilka tidskrifter som citeras ofta – representerat av storlek på noder och tidskriftstitel – dels hur tidskrifterna placeras i förhållande till varandra – baserat på hur ofta de citeras tillsammans. Citeras de ofta tillsammans placeras de närmare varandra, citeras de tillsammans mer sällan hamnar de längre ifrån varandra. Förutom samförekomster representerade genom närhet på kartan görs det också en klustringsanalys, som identifierar statistiska samband, också baserat på samförekomster. Dessa kluster representeras av olika färger. Vidare kompletteras analysen också med linjer som representerar starkare samband (mer än 1 000 co-citeringslänkar), vilket gör att man kan se i vilken utsträckning de olika klustren länkar tillsammans och – i förlängningen – i vilken utsträckning olika forskningsfält kommunicerar med varandra (se nedan).



Figur 4. Co-citerade tidskrifter.

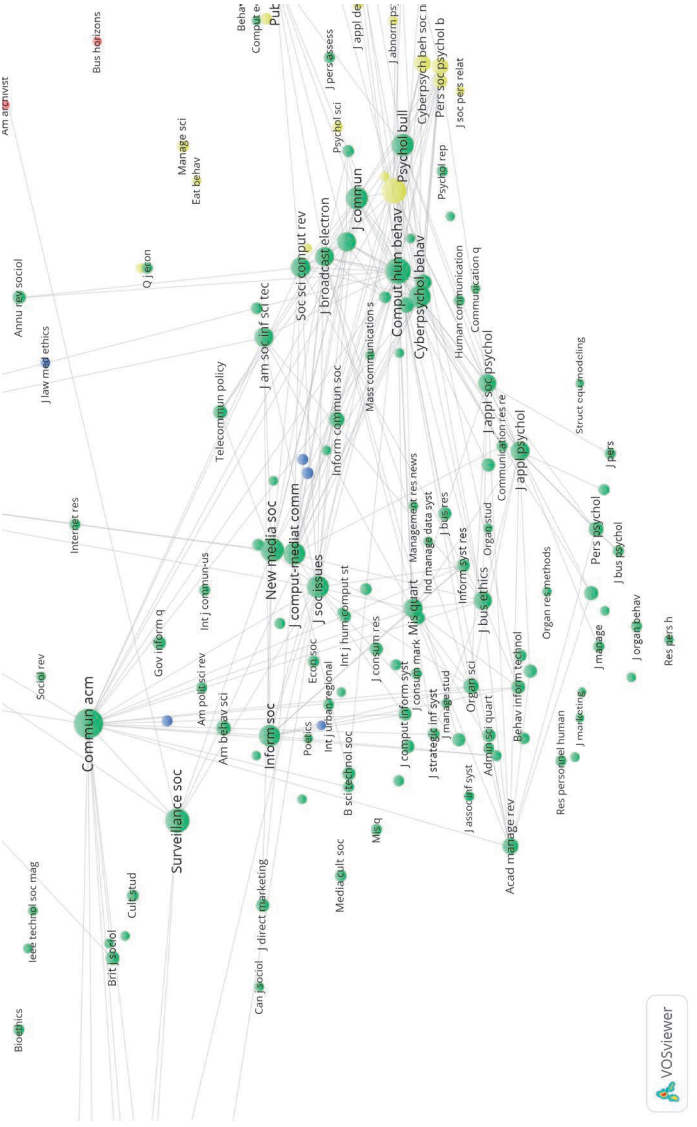
I den högra delen av kartan ovan hittar vi två kluster som framför allt innehåller den medicinskt orienterade forskningen (tillsammans med mer kliniskt orienterad psykologi och psykiatri) som återstår trots försöken att avgränsa sökningen; och som i hög grad rör t.ex. epidemiologisk forskning och forskning kring sjukdoms- och riskbeteenden (från diabetes till könssjukdomar och beroende-orienterad forskning); men också medicinsk- och beteendevetenskaplig forskning som faller inom ramen för vad som är relevant för den här studien. Till vänster på kartan hittar vi ett kluster med juridisk forskning. I den övre delen av kartans mitt finner vi datavetenskaplig

forskning, som i hög utsträckning framför allt handlar om utveckling av system och nätverk, och metoder för signal- och mönsteranalys för övervakning snarare än effekter av övervakningen på individer och frågor om integritet och dylikt (se nedan).



Figur 5. In-zoomning i karta med co-citerade tidskrifter: datavetenskapligt kluster.

Det kluster som kanske är mest intressant utifrån temat för den här studien finner vi i nedre delen av kartans mitt (se nedan). Där samlas forskning representerad av tidskrifter inom informatik, psykologi, management- & marketingforskning, sociologi och annan samhällsvetenskap, samt biblioteks- och informationsvetenskap och medie- och kommunikationsvetenskap.

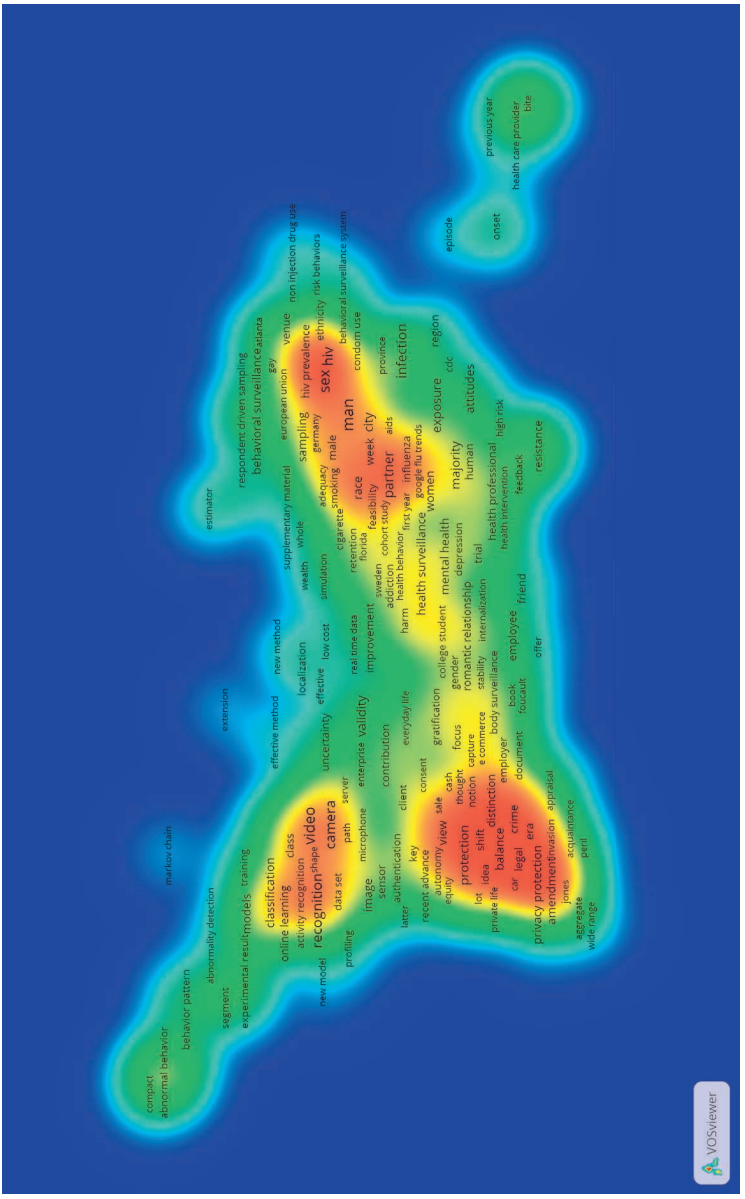


Figur 6. In-zoomning i karta med co-citerade tidskrifter: samhällsvetenskapligt kluster.

Vi kan alltså se en ganska strikt uppdelning av forskning om integritet och övervakning, med tre huvudsakliga fokus: ett tekniskt perspektiv som i hög grad handlar om systemutveckling, ett juridiskt perspektiv med fokus på frågor om lagstiftat skydd av personlig integritet, samt ett mer samhällsvetenskapligt perspektiv som bland annat samlar informatik, psykologi och marketing- och managementforskning. Mellan de olika huvudklustren är det få länkar: man skulle t.ex. kunna tänka sig starkare länkar mellan datavetenskaplig forskning om systemutveckling och den mer användarorienterade informatiken (i hög grad människa-datorinteraktionsforskning) men så är alltså inte fallet. De starkaste länkarna mellan forskningsfält finner vi inom det mer samhällsvetenskapliga klustret, där informatik, psykologi, sociologi, statsvetenskap och marketing- och managementforskning förefaller samverka över disciplinära gränser.

Analys av begrepp
För att gå vidare och identifiera inte bara inom vilka forskningsfält som integritets- och övervakningsfrågor studeras, utan också vad det är man forskar om, gjordes en motsvarande analys som – till skillnad från analysen av forskningsfält – inte bygger på samförekomster av referenser utan istället samförekomster av begrepp. Från artiklarna som identifierats i WoS-sökningen hämtades artiklarnas titlar, abstract och nyckelord som beskriver artiklarnas innehåll. Liksom i den tidigare analysen grupperas de begrepp som förekommer tillsammans i dokumenten.

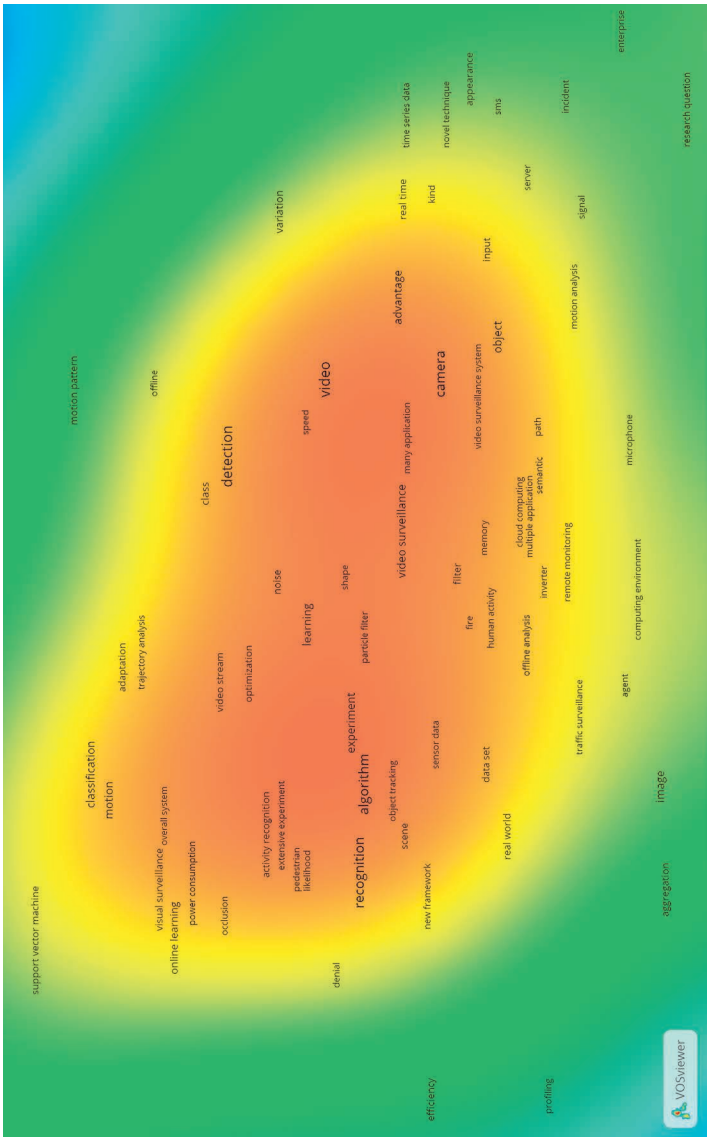
Kartan illustrerar alltså hur de 1465 begrepp som förekommer minst 2 gånger förhåller sig till varandra, de som förekommer ofta tillsammans hamnar närmare varandra på kartan, medan begrepp med lägre grad av samförekomst hamnar längre ifrån. Kartan redovisar också var man hittar större mängder begrepp med starkare samband genom att markera dessa områden med rött, medan områden med färre begrepp och med svagare samband går längre och längre mot grönt och till slut blått.



Figur 7. Samförekomst av begrepp i titlar, abstract samt nyckelord.

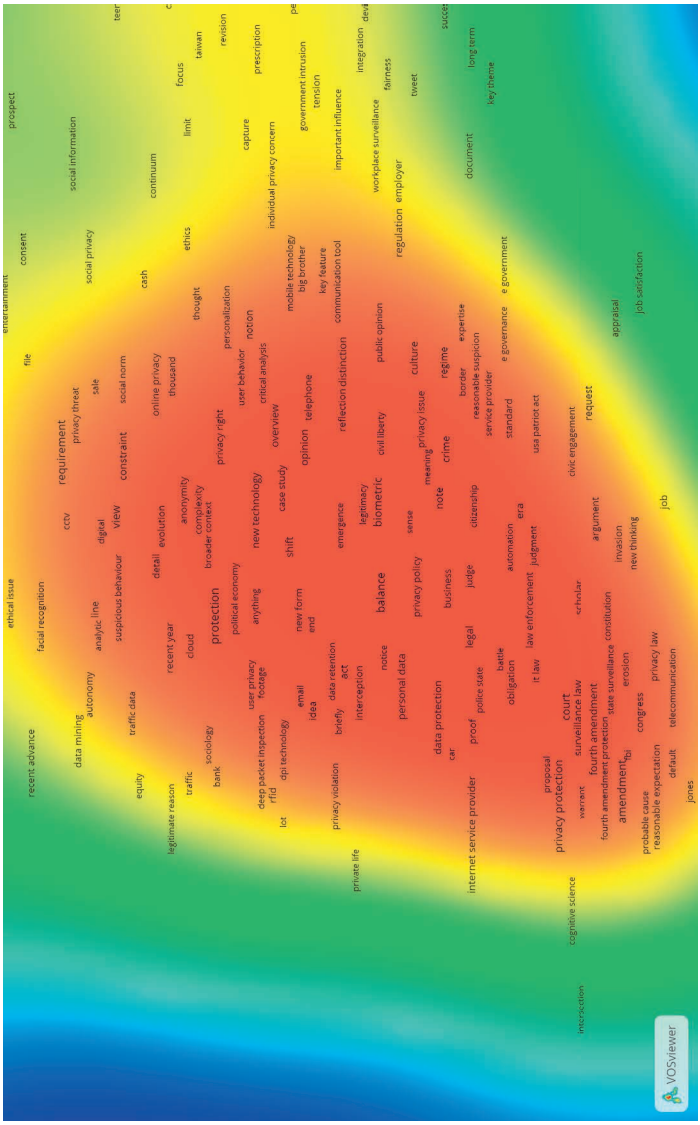
Vi kan se tre huvudsakliga kluster av begrepp på kartan (Figur 7). Till höger finner vi begrepp relaterade till den medicinska forskningen, där övervakning framför allt ska ses som en aspekt av vårdverksamhet för att övervaka eller förhindra spridande av epidemier och för att följa hälsoutveckling, snarare än som en form av kontroll av människor.

I den övre delen av kartans vänstra sida hittar vi ett kluster som motsvarar den teknikvetenskapliga forskningen vi kunde identifiera i vår analys av forskningsfält (Figur 8). Utifrån begreppen i klustret kan vi se att forskningen till stor del handlar om utveckling av system och tekniker för övervakning och igenkänning av mönster i data.



Figur 8. In-zoomning i karta med samförekommande begrepp: datavetenskapligt kluster.

I den nedre delen av kartans vänstra sida hittar vi ett kluster som verkar samla ihop de juridiska och de samhällsvetenskapliga/beteendevetenskapliga forskningsfälten från kartan över forskningsfält. Begreppen knyter an till juridiska, politiska och sociala frågor som skydd av personlig integritet, lagstiftning och förhållande till grundlagar, legitimitet, samt beteenden och sociala normer (Figur 9).



Figur 9. In-zoomning i karta med samförekommande begrepp: samhällsvetenskapligt och juridiskt kluster.

Liksom i kartan över forskningsfälten finner vi få länkar mellan de sociala/samhällsvetenskapliga aspekterna och de mer tekniskt eller medicinska aspekterna, samtidigt som vi kan se att den samhällsvetenskapliga och den juridiska forskningen här begreppsmässigt samlas inom samma kluster. Detta ska dock kanske mer ses som ett tecken på att dessa forskningsfält i hög grad använder samma – och en relativt allmän – terminologi, än att de två forskningsperspektiven aktivt kommunicerar med varandra.

Systematisk litteraturöversikt

Litteratursökningen har uteslutande fokuserat peer-reviewgranskade vetenskapliga artiklar publicerade på engelska under perioden 2005-2015. Peer-review innebär att artiklarna granskas av externa sakkunniga forskare som säkerställer att artiklarna och studierna uppfyller alla krav på vetenskaplig kvalitet. Vi har använt oss av en s.k. booelsk sökning (AND/OR/NOT). De olika databaserna har lite olika funktioner varför sökningar kommer att presenteras separat. Gränssnittet möjliggör sökningar inom antingen/och/eller abstract (AB) och ämnesområde (SU). Genom att göra sökningen i keywords ges möjligheten att fånga upp de texter där författarna själva har specificerat ett antal nyckelord för sin text. Sökningar i denna typ av ämnesord lämpar sig särskilt väl inom områden där det finns en väl etablerad terminologi och samsyn kring innebörden i olika begrepp. Alternativt kan en sökning genomföras i abstract. Detta öppnar upp för möjligheten att söka av ett lite bredare fält där det kanske används lite olika begrepp för att beskriva ungefär samma sak. Samtidigt genererar en bredare sökning ett större material som kommer att behöva avgränsas i nästa steg.

SCOPUS
Sökord och deras inbördes relation relaterar till diskussionerna avseende uppdraget, som beskrevs inledningsvis. Litteratursökningen har uteslutande fokuserat peer-reviewgranskade vetenskapliga artiklar publicerade på engelska under perioden 2005-2015. Genom att använda följande nyckelord: surveillance, internet, online, digital, behaviour, attitudes och privacy genererades följande söksträng:

TITLE-ABS-KEY (((**"Surveillance"**) AND (**"online"** OR **"digital"** OR **"Internet"**) AND (**behaviour** OR **"attitudes"** OR **"privacy"**))) AND DOCTYPE (**ar** OR **re**) AND PUBYEAR > **2004** AND (LIMIT-TO (SUBJAREA , **"SOCI"**) OR LIMIT-TO (SUBJAREA , **"COMP"**) OR LIMIT-TO (SUBJAREA , **"ENGI"**) OR LIMIT-TO (SUBJAREA , **"PSYC"**))

Sökningen genererade 342 artiklar som fördelar sig på följande sätt utifrån publiceringsår:

År	**Antal**
2015	31
2014	55
2013	54
2012	41
2011	45
2010	34
2009	20
2008	23
2007	16
2006	10
2005	13

Sökningen fördelar sig på följande sätt utifrån publikationsland (vilket inte säger något om var forskningen är utförd, eftersom forskare publicerar sig i internationella tidsskrifter):

Publiceringsländer	**Antal**
USA	139
Storbritannien	43
Australien	21
Kina	21
Kanada	19
Italien	11
Sydkorea	10
Nederländerna	9
Taiwan	9
Tyskland	9

Web of Science (core collection)
I denna databas genomfördes sökningen i ”Topic”, vilket inkluderar sökningar i Titlar, Ämnesord och Abstracts. Genom att använda följande nyckelord: surveillance, internet, online, digital, behaviour, attitudes och privacy genererades följande söksträng:

TOPIC: ((("Surveillance") AND (“online" OR "digital" OR "Internet") AND (behaviour OR ”attitudes” OR ”privacy”)))

Refined by: DOCUMENT TYPES: (ARTICLE OR REVIEW)

Vid en första genomgång av sökresultat visar det sig att många av artiklarna har ett fokus på rent medicinska frågeställningar. T ex:

Grigorescu, V. I., D'Angelo, D. V., Harrison, L. L., Taraporewalla, A. J., Shulman, H., & Smith, R. A. (2014). Implementation Science and the Pregnancy Risk Assessment Monitoring System. *Journal of Women's Health*, *23*(12), 989-994.

I syfte att utesluta denna typ av medicinska artiklar använder vi oss av funktionen ”Web of science categories” vilket möjliggör att sortera ut ett antal områden vilka bedöms irrelevanta för frågeställningen. Därmed erhålls en hanterbar mängd artiklar med relevans för uppdraget. Vi bedömer att följande kategorier av journals kan sorteras bort från sökningen:

AND [excluding] **WEB OF SCIENCE CATEGORIES:** (PERIPHERAL VASCULAR DISEASE OR INFECTIOUS DISEASES OR OPTICS OR OBSTETRICS GYNECOLOGY OR TROPICAL MEDICINE OR NUTRITION DIETETICS OR RESPIRATORY SYSTEM OR PARASITOLOGY OR FOOD SCIENCE TECHNOLOGY OR VETERINARY SCIENCES OR UROLOGY NEPHROLOGY OR MEDICINE GENERAL INTERNAL OR SURGERY OR ENDOCRINOLOGY METABOLISM OR CLINICAL NEUROLOGY OR MEDICINE RESEARCH EXPERIMENTAL OR IMMUNOLOGY OR GENETICS HEREDITY OR DERMATOLOGY OR TOXICOLOGY OR GASTROENTEROLOGY HEPATOLOGY OR

PEDIATRICS OR RADIOLOGY NUCLEAR MEDICINE MEDICAL IMAGING OR FISHERIES OR ONCOLOGY OR ZOOLOGY OR PHARMACOLOGY PHARMACY OR CHEMISTRY ANALYTICAL)
Timespan: 2005-2015. **Indexes:** SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.

Resultatet efter automatiserad exkludering blev **330** artiklar, som fördelar sig enligt följande (av databasen angivna områden):

Områden	**Antal**
COMPUTER SCIENCE	63
PSYCHOLOGY	47
PUBLIC ENVIRONMENTAL OCCUPATIONAL HEALTH	43
GOVERNMENT LAW	37
INFORMATION SCIENCE LIBRARY SCIENCE	31
ENGINEERING	30
COMMUNICATION	23
SOCIAL SCIENCES OTHER TOPICS	22
HEALTH CARE SCIENCES SERVICES	22
SCIENCE TECHNOLOGY OTHER TOPICS	18

Publiceringsländer	**Antal**
USA	174
ENGLAND	40
AUSTRALIA	27
CANADA	17
ITALY	16
PEOPLES R CHINA	12
NEW ZEALAND	8
TAIWAN	7
SOUTH KOREA	7
NETHERLANDS	7

År	**Antal**
2015	72
2014	43
2013	42
2012	41
2011	39
2010	30
2008	17
2009	16
2007	13
2006	11

Extrahering och värderingen av materialet

De sammanlagt 672 artiklar, som sökts ut enligt tidigare formulerade kriterier och databaser, importerades sedan och sorteras i referenshanteringssystemet Mendeley. Här genomförs följande sortering.

En första sållning handlar om att ta bort dubletter. Efter utsortering av dubbletter (147 st) fanns 525 artiklar kvar. Därefter sorteras artiklar bort som inte är publicerade på engelska (6 st) varefter det fanns 519 artiklar kvar. På basis av att titlarna inte bedömdes som ämnesrelevanta sorterades sedan 70 artiklar bort, vilket innebar att det efter en första sållning fanns 449 artiklar kvar. Samtliga 449 abstracts skrevs sedan ut och genomgick närläsning. En ny utsortering genomförs enligt följande kategorier:

Y (icke ämnesrelevant) = 260 artiklar sorterades ut.
X (icke en peer-reviewgranskad vetenskaplig artikel) = 17 artiklar sorterades ut.

Kvar blev 172 artiklar kvar för analys. Dessa artiklar lästes i fulltext och kategoriserades av oss utifrån forskningsfokus och studieobjekt. Följande områden identifierades (antalet artiklar anges inom parantes).

Teknik (27)
Lagstiftning (25)
Stat (23)
Generella teoretiska resonemang (21)
Arbete (12)
Kunskap och beteende bland unga (17)
Hälsa (14)
Handel (12)
Privata relationer (9)
Mänskliga rättigheter i det digitala (4)
Sousveillance (3)
Övrigt (5)

Nedan följer en genomgång av respektive fält.

Teknik

27 artiklar

På generellt plan är de artiklar som beskriver den tekniska sidan av övervakning på Internet övervägande utvecklings- och lösningsorienterade. D.v.s. de handlar om hur vi med teknikens hjälp kan utveckla Internet i riktning mot bättre användarvänlighet och integritetsskydd. Begrepp som syftar till att beskriva hur skydd för integriteten kan ”byggas in” i tekniken är ”Trusted computing” (Shiguo et al. 2009; Winkler och Renner 2011), ”Privacy aware design” (Wicker 2011) samt ”Privacy by design” (Cavoukian et al. 2012). Undantagsvis förekommer det artiklar (McKee 2011; Mitchelfelder 2009 och Vitaliev 2007), vilka anlägger ett mer kritiskt perspektiv och lyfter fram det hot som tekniken kan medföra för den personliga integriteten och rätten till privatliv. I syfte att öka medvetenheten och för att komma tillrätta med integritetsfrågor på nätet formuleras följande upprop av McKee (2011, s 287):

”We can change the settings on the software and hardware on our computers and mobile devices (e.g, blocking cookies, turning off location services). We can learn about the specific privacy policies of various sites we use and take action to change our privacy settings. We can find out from some corporations what our behavioral profile is, and we can choose to opt-out of targeted, personalized advertising, either on a site-by-site and company basis or, if the do-not-track option becomes available, then more widely across all the sites we visit. We can choose not to use some sites that have more egregious records of privacy violations. And we can learn more about and use more open-source, non-commercial sites and applications, either those online or ones to be downloaded and hosted on local servers.”

I relation till denna utveckling, mot en teknik som i allt större utsträckning utsätter individens integritet för hot, formulerar även Wicker och Schrader (2011, s 330) ett upprop riktat mot alla ingenjörer att motarbeta utvecklingen: ”Engineers and computer scientists thus have a moral obligation to avoid design choices that are unnecessarily privacy invasive.” De principer som borde vägleda arbetet med att utforma de tekniska aspekterna av framtidens Internet formuleras i termer av ”Privacy-Aware Design Principles” och omfattar fem punkter vilka är tänkta att öka såväl transparans avseende vad som samlas in som möjligheten att påverka vilken information som samlas in:

1) Provide full disclosure of data collection
2) Require consent to data collection
3) Minimize collection of personal data
4) Minimize identification of data with individuals
5) Minimize and secure data retention

På liknande sätt diskuterar Winkler och Renner (2011) hur integritet kan skyddas i termer av ”trusted computing”. Mer specifikt behandlar artikeln videoövervakning av offentliga miljöer i syfte att förebygga brott, samt i relation till detta olika tekniker för att spara och behandla potentiellt integritetskänslig information som genereras genom övervakningen. Det är i detta sammanhang värt att påpeka att gränsen mellan videoövervakning och

övervakning i det digitala blir allt otydligare och teknikerna går in i varandra. Artikeln diskuterar ett antal olika förhållningssätt, t.ex. att data som genereras separareras på ett sätt så att personlig information skiljs från information om beteende: ”personal and behavioral data should be separated directly on the camera. While system operators only get access to behavioral data, a separate stream containing personal data is made available to law enforcement authorities.” alterntativt att bildinformation som kan röja identiteten på en individ automatiskt tas bort genom en s k ”Respectful camera” som detects and blanks people's faces in captured images”. Här beskrivs även ett kryptograferingsverktyg ”PICO” vilket skulle kunna användas för att kryptera integritetskänslig information och där avkryptering av insamlat material endast kunde ske efter det att ett brott begåtts (Winkler och Renner 2011, s 17). Även Babaguchi och Nakashima (2015) behandlar frågan om hur potentiellt integritetskänslig information som samlas in genom videoövervakning kan hanteras. I deras artikel behandlas ett antal konkreta projekt som alla (PriSurv, Digital Diorama (DD), and Mobile Privacy Protection (MPP)) som alla syftar till att stärka individers rätt till privatliv. Ett annat begrepp som förkommer i detta sammanhang är ”Privacy by design” (PbD) där frågor om integritet ”is embedded as a core functionality in the biometric system” Cavoukian et al. (2012). Författarna argumenterar för att frågor om integritet bör utgöra utgångspunkten i arbetet med utvecklingen av ny teknik och nya affärsmodeller, istället för att behandlas i slutskedet eller inte alls.

PbD återkommer även i Shilton (2012) som först och främst behandlar frågan om integritetsfrågor relaterat till användargenerad data. Artikeln beskriver utvecklingen mot att individer genom appar och wearables mäter och kommunicerar t ex motions-, mat- och sömnvanor i sociala nätverk. PbD kan i detta sammanhang innebära att i utvecklingsfasen av denna typ av produkter och tjänster tydligare fokusera hur potentiellt integritetskänslig information kan och bör hanteras. T ex att tydliggöra vilken information som samlas in, men även att underlätta för användaren att själv kunna ställa in hur information samlas, men även hur den kommuniceras.

Shiguo et al. (2009) beskriver den senaste teknikutvecklingen inom området multimedia, vilket inbegriper användarinformation som sparas i samband med vissa tv-tjänster online. Vidare diskuteras olika möjligheter att skydda och hantera känslig information genom t ex olika former av krypteringssystem.

Utifrån ett historiskt perspektiv beskriver Estee (2015) framväxten av olika tekniker för att spåra användares beteende på Internet, från 1990-talet och fram till idag. Med ett särskilt fokus på webbkakor ”cookies” (vilka är textbaserade datafiler med information om användaren som sparas på webbplatsbesökarens dator), hur dessa vuxit fram i olika former samt vilka tekniker som formerats i relation till detta för att skydda användarens integritet. I artikeln lyfts behovet fram av att informera och upplysa ungdomar och studenter om tekniken. I det avslutande kapitlet ”Taking back our digital identities” kan man läsa: ”The implications concern how everyone can continue to interact in online spaces in safe ways and understand how our invisible digital identities are constructed through surfing habits. Those implications include responsibilities to act and teach students about how to protect their identities online. It is up to all of us, as teachers and researchers,

to talk about invisible digital identities with each other and our students." (Estee 2015, s 130).

Andrejevic, M., & Burdon, M. (2015). Defining the Sensor Society. *TELEVISION & NEW MEDIA*, *16*(1, SI), 19–36. http://doi.org/10.1177/1527476414541552

Asiaghi, A. (2009). Materialized surveillance. *Mechanical Engineering*, *131*(3). Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-67650751638&partnerID=tZOtx3y1

BABAGUCHI, N., & NAKASHIMA, Y. (2015). Protection and Utilization of Privacy Information via Sensing. *IEICE Transactions on Information and Systems*, *E98.D*(1), 2–9. http://doi.org/10.1587/transinf.2014MUI0001

Beck, E. N. (2015). The Invisible Digital Identity: Assemblages in Digital Networks. *Computers and Composition*, *35*, 125–140. http://doi.org/10.1016/j.compcom.2015.01.005

Cavoukian, A., Chibba, M., & Stoianov, A. (2012). Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment. *REVIEW OF POLICY RESEARCH*, *29*(1), 37–61. http://doi.org/10.1111/j.1541-1338.2011.00537.x

Chang, R.-I., Wang, T.-C., Wang, C.-H., Liu, J.-C., & Ho, J.-M. (2012). Effective distributed service architecture for ubiquitous video surveillance. *INFORMATION SYSTEMS FRONTIERS*, *14*(3), 499–515. http://doi.org/10.1007/s10796-010-9255-z

Conti, M., Zhang, L., Roy, S., Di Pietro, R., Jajodia, S., & Mancini, L. V. (2009). Privacy-preserving robust data aggregation in wireless sensor networks. *Security and Communication Networks*, *2*(2), 195–213. http://doi.org/10.1002/sec.95

Doyle, T., & Veranas, J. (2014). Public anonymity and the connected world. *ETHICS AND INFORMATION TECHNOLOGY*, *16*(3), 207–218. http://doi.org/10.1007/s10676-014-9346-5

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–15. http://doi.org/10.1007/s11948-014-9551-y

Foresti, G. L., Micheloni, C., Piciarelli, C., & Snidaro, L. (2009). Visual sensor technology for advanced surveillance systems: historical view, technological aspects and research activities in Italy. *Sensors (Basel, Switzerland)*, *9*(4), 2252–70. http://doi.org/10.3390/s90402252

Fuchs, C. (2013). SOCIETAL AND IDEOLOGICAL IMPACTS OF DEEP PACKET INSPECTION INTERNET SURVEILLANCE. *INFORMATION COMMUNICATION & SOCIETY*, *16*(8), 1328–1359. http://doi.org/10.1080/1369118X.2013.770544

H. Dutton, W. (2014). Putting things to work: social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. http://doi.org/10.1108/info-09-2013-0047

Hossain, M. A. (2014). Framework for a Cloud-Based Multimedia Surveillance System. *International Journal of Distributed Sensor Networks*, *2014*, 1–11. http://doi.org/10.1155/2014/135257

Kim, H., Giacomin, J., & Macredie, R. (2014). A Qualitative Study of Stakeholders' Perspectives on the Social Network Service Environment. *International Journal of Human-Computer Interaction*, *30*(12), 965–976. http://doi.org/10.1080/10447318.2014.925383

Leo, M., D'Orazio, T., Caroppo, A., Martiriggiano, T., & Spagnolo, P. (2005). Automatic monitoring of forbidden areas to prevent illegal accesses. In P. Singh, S and Singh, M and Apte, C and Perner (Ed.), *PATTERN RECOGNITION AND IMAGE ANALYSIS, PT 2, PROCEEDINGS* (Vol. 3687, pp. 635–643).

McKee, H. A. (2011). Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance. *Computers and Composition*, *28*(4), 276–291. http://doi.org/10.1016/j.compcom.2011.09.001

Michelfelder, D. P. (2009). Philosophy, privacy, and pervasive computing. *AI & SOCIETY*, *25*(1), 61–70. http://doi.org/10.1007/s00146-009-0233-2

Moradoff, N. (2010). Biometrics: Proliferation and constraints to emerging and new technologies. *SECURITY JOURNAL*, *23*(4), 276–298. http://doi.org/10.1057/sj.2008.21

Mordini, E., & Rebera, A. P. (2012). No Identification Without Representation: Constraints on the Use of Biometric Identification Systems. *REVIEW OF POLICY RESEARCH*, *29*(1), 5–20. http://doi.org/10.1111/j.1541-1338.2011.00535.x

Morris, B. T., & Trivedi, M. M. (2011). Trajectory learning for activity understanding: unsupervised, multilevel, and long-term adaptive approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *33*(11), 2287–301. http://doi.org/10.1109/TPAMI.2011.64

Nguyen, H. T. M. (2011). CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING. *NOTRE DAME LAW REVIEW*, *85*(6), 2189–2218.

Shiguo, L., Kanellopoulos, D., & Ruffo, G. (2009). Recent advances in multimedia information system security. *Informatica (Ljubljana)*, *33*(1), 3–24. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-64249107623&partnerID=tZOtx3y1

Shilton, K. (2012). Participatory personal data: An emerging research challenge for the information sciences. *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY*, *63*(10), 1905–1915. http://doi.org/10.1002/asi.22655

Vitaliev, D. (2007). Big brother is watching you [Internet security]. *Communications Engineer*, *5*(5), 20–25. http://doi.org/10.1049/ce:20070502

Weaver, S. D., & Gahegan, M. (2007). Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*, *97*(3), 324–350. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-36849064241&partnerID=tZOtx3y1

Wicker, S. B., & Schrader, D. E. (2011). Privacy-Aware Design Principles for Information Networks. *Proceedings of the IEEE*, *99*(2), 330–350. http://doi.org/10.1109/JPROC.2010.2073670

Winkler, T., & Rinner, B. (2011). Securing Embedded Smart Cameras with Trusted Computing. *EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING*. http://doi.org/10.1155/2011/530354

Lagstiftning

25 artiklar

På ett övergripande plan behandlar i princip samtliga artiklar rättens oförmåga att skydda individens rättigheter till följd av snabba framväxten av digital teknologi. En central fråga, för de artiklar som rör förhållanden i USA, avseende legala av aspekter av den digitala tekniken och hot om att inskränka den personliga integriteten, är ”the Fourth Amendment” (Desai 2014; Hu 2013; Kerr 2010; Solove 2005); som utgör en viktig del av den amerikanska konstitutionen. Den del av Fourth amendment som diskuteras i detta sammanhang rör individens rätt till privatliv. Utgångspunkten i samtliga artiklar är antagandet att den digitala teknikutvecklingen medfört att lagen inte längre på ett fullgott sätt förmår att skydda individens rätt till privatliv.

Kerr (2010) söker att applicera konstitutionen och the Fourth Amendment på en Internet-relaterad kontext och tar sin utgångspunkt i de otydligheter som existerar avseende vilken typ av digital kommunikation (t ex e-post och sms) som skyddas från övervakning av lagen. Ambitionen är att söka skapa ett system som ger ett lika stort skydd i den digitala världen som i den fysiska. Mer specifikt diskuterats distinktionen mellan ”Inside” och ”Outside” i en polisundersökning. Termerna beskriver individens förväntningar på privatliv och polisens rättigheter att observera och samla in information om individers beteende, i relation till vilken fysisk miljö individen befinner sig i. Lagen gör skillnad på rätt till privatliv beroende av huruvida du rör dig i ett offentligt utrymme eller i ditt eget hus. Frågan som diskuteras i artikeln är följaktligen hur denna distinktion ska översättas i en digital kontext.

Även Desai (2014) diskuterar individens rätt till privatliv i relation till polisutredningar men i termer av ”Forward looking” och ”Backward looking” övervakning. Forward looking övervakning beskriver den typ av övervakning som sker med ett speciellt tillstånd av en domare och omfattar t ex GPS-övervakning och telefonavlyssning. För att få till stånd ett sådant krävs misstanke om någon form av kriminell handling. Vidare anger tillståndet vilken typ av information som får samlas in samt i vilket syfte den kan användas. Problemet som diskuteras i artikeln avser backward looking vilket beskrivs på följande sätt: ” With backward-looking surveillance all these protections are gone. Law enforcement or intelligence services need only ask a business for the record of where we went, whom we called, what we read, and more. They then have a near perfect picture of our activities and associations regardless of whether they are criminal. There is thus an asymmetry that makes little sense.” (Desai 2014, s. 582-583). Framförallt beskrivs detta sätt att tämligen enkelt skapa en detaljerad bild över en individs liv vara ett hot mot att organisera och uttrycka sig politiskt.

Ett annat centralt tema i de artiklar som behandlar lagstiftning är rätten till data (Cover 2015; Grodzinsky och Tavani 2005; Konstadinides 2011; Mantalero 2014; Peppet 2014; Roberts 2015). Utgångspunkten är den oklarhet som råder avseende vem som äger information som genereras när man agerar på nätet, samt vem som har rätt till dessa data och i vilket syfte den får användas. Mantelero (2014, s. 644) formulerar problematiken på följande sätt: ”However, the high demand for personal information, the

complexity of the new tools of analysis and the increasing numbers of sources of data collection, have generated an environment in which the 'data barons' (i.e. big companies, government agencies, intermediaries) have a control over digital information which is no longer counterbalanced by the user's self-determination." Den lagstiftning som är tänkt att skydda individens rätt till integritet i sammanhanget bygger på principen "Notice and consent", d.v.s. användaren ska ha rätt till att bli informerad om vilken data som samlas in och även ha möjlighet att ge samtycke eller ej. Problem med Notice and consent i detta sammanhang beskriver Mantelero (2014, s. 652) som: "Since Big Data analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, the description of these purposes is becoming more and more "evanescent". This is a consequence of the "transformative" use of Big Data, which makes it often impossible to explain all the possible uses of data at the time of its initial collection." Med andra ord har den så kallade handeln med data inneburit att den hamnar i nya sammanhang än vad som från början var avsett. Detta i kombination med att data från olika sammanhang sammanförs och analyseras kan mönster om såväl individer som grupper avtäckas. Peppet (2014) adresserar framväxten av "Internet of things" samt potentiella problem med hur data lagras och används i detta sammanhang. Internet of things är en samlingsterm för datorbaserad teknik inbyggd i produkter (ofta bärbara) som registrerar vardagliga aktiviteter såsom motions-, mat- och sömnvanor. I detta sammanhang frågar sig författaren "As the Internet of Things generates ever more massive and nuanced datasets about consumer behavior, how to protect privacy? How to deal with the reality that sensors are particularly vulnerable to security risks? How should the law treat and how much should policy depend upon consumer consent in a context in which true informed choice may be impossible?" (Peppet 2014, s. 85).

Brown, I. (2010). Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, *19*(2), 95–109. http://doi.org/10.1093/ijlit/eaq016

Cheng, F.-C., & Lai, W.-H. (2010). An overview of VoIP and P2P copyright and lawful-interception issues in the United States and Taiwan. *Digital Investigation*, *7*(1-2), 81–89. http://doi.org/10.1016/j.diin.2010.08.001

Coudert, F. (2009). Towards a new generation of CCTV networks: Erosion of data protection safeguards? *Computer Law & Security Review*, *25*(2), 145–154. http://doi.org/10.1016/j.clsr.2009.02.003

Cover, A. Y. (2015). Corporate Avatars and the Erosion of the Populist Fourth Amendment. *IOWA LAW REVIEW*, *100*(4), 1441–1502.

Desai, D. R. (2014). CONSTITUTIONAL LIMITS ON SURVEILLANCE: ASSOCIATIONAL FREEDOM IN THE AGE OF DATA HOARDING. *NOTRE DAME LAW REVIEW*, *90*(2), 579–632.

Fairfield, J. A. T., & Luna, E. (2014). DIGITAL INNOCENCE. *CORNELL LAW REVIEW*, *99*(5), 981–1076.

Garlinger, P. P. (2009). PRIVACY, FREE SPEECH, AND THE PATRIOT ACT: FIRST AND FOURTH AMENDMENT LIMITS ON NATIONAL SECURITY LETTERS. *NEW YORK UNIVERSITY LAW REVIEW*, *84*(4), 1105–1147.

Grodzinsky, F. S., & Tavani, H. T. (2005). P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property. *Ethics and Information Technology*, *7*(4), 243–250. http://doi.org/10.1007/s10676-006-0012-4

Hayes, A. S. (2014). The USPS as an OSP: A Remedy for Users' Online Privacy Concerns. *Communication Law and Policy*, *19*(4), 465–507. http://doi.org/10.1080/10811680.2014.955770

Hu, M. (2013). Biometric ID Cybersurveillance. *INDIANA LAW JOURNAL*, *88*(4), 1475–1558.

Kerr, O. S. (2010). APPLYING THE FOURTH AMENDMENT TO THE INTERNET: A GENERAL APPROACH. *STANFORD LAW REVIEW*, *62*(4), 1005–1049.

Kierkegaard, S. (2005). Privacy in electronic communication. *Computer Law & Security Review*, *21*(3), 226–236. http://doi.org/10.1016/j.clsr.2005.04.008

Konstadinides, T. (2011). Destroying democracy on the ground of defending It? the Data Retention Directive, the surveillance state and our constitutional ecosystem. *European Law Review*, *36*(5), 722–736. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84868150276&partnerID=tZOtx3y1

Mantelero, A. (2014). The future of consumer data protection in the EU Re-thinking the ``notice and consent{''} paradigm in the new era of predictive analytics. *COMPUTER LAW & SECURITY REVIEW*, *30*(6), 643–660. http://doi.org/10.1016/j.clsr.2014.09.004

Nguyen, H. T. M. (2011). CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING. *NOTRE DAME LAW REVIEW*, *85*(6), 2189–2218.

Ojanen, T. (2014). Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Right. *EUROPEAN CONSTITUTIONAL LAW REVIEW*, *10*(3), 528–541. http://doi.org/10.1017/S1574019614001345

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *TEXAS LAW REVIEW*, *93*(1), 85–178.

Riedy, M. K., & Wen, J. H. (2010). Electronic surveillance of Internet access in the American workplace: implications for management. *Information & Communications Technology Law*, *19*(1), 87–99. http://doi.org/10.1080/13600831003726374

Roberts, A. (2015). Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. *MODERN LAW REVIEW*, *78*(3), 535–548. http://doi.org/10.1111/1468-2230.12127

Robison, W. J. (2010). Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act. *GEORGETOWN LAW JOURNAL*, *98*(4), 1195–1239.

Saxby, S. (2014). The 2013 CLSR-LSPI seminar on electronic identity: The global challenge - Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11-15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand. *COMPUTER LAW & SECURITY REVIEW*, *30*(2), 112–125. http://doi.org/10.1016/j.clsr.2014.01.007

Schlabach, G. R. (2015). PRIVACY IN THE CLOUD: THE MOSAIC THEORY AND THE STORED COMMUNICATIONS ACT. *STANFORD LAW REVIEW*, *67*(3), 677–721.

Solove, D. J. (2005). Fourth Amendment codification and Professor Kerr's misguided call for judicial deference. *FORDHAM LAW REVIEW*, *74*(2), 747–777.

Stalla-Bourdillon, S. (2013). Online monitoring, filtering, blocking ….What is the difference? Where to draw the line? *Computer Law & Security Review*, *29*(6), 702–712. http://doi.org/10.1016/j.clsr.2013.09.006

Stalla-Bourdillon, S., Papadaki, E., & Chown, T. (2014). From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy … The case of deep packet inspection technologies. *Computer Law & Security Review*, *30*(6), 670–686. http://doi.org/10.1016/j.clsr.2014.09.006

Stat

23 artiklar

Gemensamt för de artiklar som behandlar frågan om relationen mellan stat och medborgare i en digital kontext är hur och i vilka sammanhang det kan betraktas som legitimt för staten att aktivt samla in information avseende individers kommunikation på Internet, samt vilka konsekvenserna kan tänkas bli i termer av bristande tillit och politiskt engagemang när övervakningen upplevs som obefogad eller alltför långtgående. De svar som forskningen ger inom detta område är dock inte helt samstämmiga utan kräver att man tar hänsyn till enskilda länders specifika förhållanden samt interaktionen mellan upplevd nytta med övervakning och ålder, utbildning, yrke och politiska åsikter.

I fallet Kina där den totalitära enpartistaten i sig, ur ett rent demokratiperspektiv, är illegitim diskuteras frågor om övervakning som rena maktmedel för att stärka statens ställning visavi medborgarna (Jiang och Okamoto 2014; Wang och Hong 2010). I en av artiklarna (Jiang och Okamoto 2014) beskrivs att av Kinas sammanlagt 1,3 miljarder invånare är 42 % internetanvändare. Hos dessa 591 miljoner internetanvändare är web-sökningar genom olika sökmotorer en av de vanligaste aktiviteterna. Jiang och Okamotos (2014) artikel fokuserar den statliga sökmotorn Jike, vilken beskrivs av författarna som ett försök av Kinas kommunistiska parti (KKP) ”to control information, enhance legitimacy and achieve cyber power through both technological regulation and creation” (s 100). Enligt artikelförfattarna uppnås ”cyber power” genom att (1) förstärka nationell identitet och solidaritet genom sökmotorns nationalistiska gränssnitt (2) genom vilka sökresultat som förmedlas, samt (3) genom dess potential att spionera på hur användarna beter sig på nätet. De första två punkterna beskrivs tämligen ingående i artikeln emedan frågan om hur information om sökmotorns användare lagras och används diskuteras på en mer hypotetisk nivå. Detta då det inte, enligt författarna, är känt vilken typ av information som lagras samt hur denna används.

Wang och Hong (2010) fokuserar den Kinesiska bloggsfären utifrån frågor om huruvida detta forum för kommunikation möjligtvis kan bidra till en ökad öppenhet i landet. Författarna utmanar bilden av bloggar och bloggare som samhällsomvandlare och menar att den kinesiska staten framgångsrikt begränsat vad som kan uttryckas i detta medium. ”The expansion of China’s use of cyberspace is matched by the government’s efforts to control, censor, and repress it with strict legislation, jailing cyber-dissidents, spying on discussions, filtering content, and barring access to websites with the help from the Western companies who provide the mechanism through the open market. Although China’s Bloggers are empowered by this new communication vehicle, which allows them to express themselves freely and deliberately, China’s blogosphere is not leading to the overthrow of the dictatorship (s. 76).

Artiklarna som diskuterar förhållandena i Kina är starkt kritiska till landets regim och ett underliggande antagande som är genomgående är att

övervakning av medborgare på Internet i huvudsak syftar till att stärka KKPs makt och inte till att skydda medborgarna mot yttre hot.

Frågan om yttre hot samt statens möjlighet att förebygga dessa genom övervakning på Internet är ett tydligt tema också för den forskning och de artiklar som behandlar medborgare-stat i USA. Utgångspunkten i Redick et al. (2015) är den debatt som uppstod avseende den massövervakning som utförs av National Security Agency (NSA), vilken i stora delar skedde utan medborgarnas vetskap. Ett underliggande antagande i denna artikel är att övervakningen i sig är legitim och syftar till att förbättra statens funktionsförmåga: "public sector organizations are increasingly using data to improve their performance, provide greater citizen engagement, and cultivate levels of collaboration and transparency." (s. 129). Utgångspunkten är med andra ord att långtgående övervakning av medborgarna var (och är) legitim, samt att utmaningen snarare handlar om att förbättra hur övervakningsprogrammen kommuniceras: "These findings indicate that government needs to be more efficacious in communicating about surveillance programs more transparently to garner greater citizens' approval for its surveillance programs" (s. 138).

Följaktligen kommer attityden till övervakning att påverkas av i vilken mån den upplevs som legitim. Legitimiteten i sig är sin tur relaterat till upplevd hotbild samt statens förmåga att genom övervakning av medborgare förebygga och bemöta dessa hot. En slutsats som formuleras av Dinev et al. (2008, s. 214) "The perceived need for government surveillance was negatively related to privacy concerns and positively related to willingness to disclose personal information." Bilden av att det finns en tämligen långtgående acceptans för statlig övervakning i USA stärks även i Dinev et al. (2006), som genomfört en komparativ studie över attityder till övervakning mellan Italien och USA. Författarna konkluderar att "Italians exhibit lower Internet privacy concerns than individuals in the U.S., lower perceived need for government surveillance, and higher concerns about government intrusion. (s 1)". Italienarnas motvilja till statlig övervakning förklaras i artikeln dels genom en lägre upplevd risk men även med en lägre grad av tillit till staten.

I två studier avseende medborgarnas syn på statlig övervakning på Internet i Balkanländerna (Budak et al. 2013; Budak et al., 2015) visar på vikten av att ta hänsyn till olika demografiska förhållanden för att kunna förstå och förklara attityder till övervakning. I deras analys kan medborgarna delas in i tre grupper: "(1) pro-surveillance oriented citizens, (2) citizens concerned about being surveilled and (3) citizens opting for better data protection" (s 17). Dessa grupper skiljer sig åt beroende av ålder, utbildning och yrke. Exempelvis visar den statistiska analysen att medborgare med en lägre utbildningsnivå tenderade att vara mer "pro-surveillance" än de med högre utbildning. På samma sätt visar det sig sig att de som står utanför arbetsmarknaden tenderade att vara för övervakning i större utsträckning än de som lönearbetade. Vad gäller ålder visar det sig att yngre medborgare var "pro-surveillance" i större utsträckning än äldre. Samtidigt uttrycker även gruppen yngre viss oro för risken att vara övervakad.

Cohrs et al. (2005) fördjupar förståelsen för hur upplevelsen av yttre hot påverkar attityder till övervakning. Här argumenteras delvis mot Redik et al.

(2015) och Cohrs et al. (2005) menar att enbart upplevelse av hot inte nödvändigtvis påverkar attityder till övervakning.

En annan central fråga som avhandlas i de artiklar som diskuterar relationen mellan stat och medborgare är huruvida upplevelsen av att vara övervakad på Internet påverkar det politiska engagemanget. Här är resultaten tämligen motstridiga. Best och Krueger (2008) argumenterar för att rädslan för övervakning är ett reellt hot mot demokratin i det att det påverkar det politiska engagemanget. ”The findings suggest that the prospects of govemment surveillance may, in fact, be a consideration in U.S. citizens' decisions to participate politically. Concerned that the government may monitor such nonviolent activities, citizens may choose to avoid them, particularly compared to more anonymous political activities such as voting. Moreover, those who disapprove of the president are more likely to perceive govemment monitoring and are more likely to perceive that the govemment uses comparatively invasive techniques when monitoring. Therefore any ‘chilling effect’ would not be distributed randomly across the political spectrum, which potentially damages the often-cited ideal of equal consideration.” (Best och Krueger 2008, s 205).

Det finns dock studier som visar upp delvis motsatta resultat. Krueger (2005) visar att det största politiska engagemanget online uppvisar de grupper som upplever störst problem med hot om statlig övervakning. ”Those most out of step with dominant opinion, who also feel that the government monitors citizens’ Internet activity, participate in politics online at the highest rates.” Krueger (2005, s 448).

Ett upplevt hot om övervakning och bristande tillit till statens förmåga att hantera känslig information om medborgarna är även en central fråga inom området E-förvaltning (E-government). E-förvaltning är ett samlingsbegrepp för statens arbete att, med hjälp av informations och kommunikationsteknologi, förenkla och förbättra samhällsservicen till medborgare och företag samt att underlätta för medborgare att få tillgång till information och aktivt delta i beslutsprocesser i den offentliga förvaltningen. Rädslan för hur staten använder personlig och känslig information som genereras av medborgarna på Internet kan påverka tilliten mellan parterna och i förlängningen viljan att använda sig av olika e-tjänster. Detta är budskapet i Keymolen et al. (2012) som inte redovisar någon egen data, utan för diskussioner på ett mer teoretiskt plan, samt går igenom mer konkreta exempel på saker att ta hänsyn till, för att stärka tilliten mellan stat och medborgare, samt i förlängningen öka viljan att ta del av digitala tjänster och dela med sig av känslig information online. Lips (2010) argumenterar för att det finns en betydande acceptans, vad gäller att dela med sig av personlig information till staten, så länge detta leder till bättre samhällstjänster. För att detta utbyte mellan information om medborgarna och samhällstjänster ska fungera smidigt måste transparensen öka avseende vilken information som samlas in samt i vilket syfte den används. Haikola och Jonsson (2007) presenterar en studie över hur debatten fördes i Sveriges riksdag avseende relation mellan individens rätt till integritet och behovet av övervakning vid tiden för Internets framväxt. De argumenterar för att även om röster mot ökad övervakning förkom var de ändå i minoritet i relation till den rådande diskursen som inbegrep en bild om ett ökat behov av insamling av information gällande medborgarna.

Bedi, M. (2014). SOCIAL NETWORKS, GOVERNMENT SURVEILLANCE, AND THE FOURTH AMENDMENT MOSAIC THEORY. *BOSTON UNIVERSITY LAW REVIEW*, *94*(6), 1809–1880.

Best, S. J., & Krueger, B. S. (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology & Politics*, *5*(2), 191–212. http://doi.org/10.1080/19331680802294479

Budak, J., Anic, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH*, *26*(1-2, SI), 100–118. http://doi.org/10.1080/13511610.2013.723404

Budak, J., Rajh, E., & Anic, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *JOURNAL OF BALKAN AND NEAR EASTERN STUDIES*, *17*(1), 29–48. http://doi.org/10.1080/19448953.2014.990278

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 118–128. http://doi.org/10.1016/j.giq.2015.01.002

Cheng, F. C., & Lai, W. H. (2012). The observation of regulatory approach within internet activities in the United States. *International Journal of Advancements in Computing Technology*, *4*(15), 421–428. http://doi.org/10.4156/ijact.vol4.issue 15.49

Cheng, F.-C., & Lai, W.-H. (2010). An overview of VoIP and P2P copyright and lawful-interception issues in the United States and Taiwan. *Digital Investigation*, *7*(1-2), 81–89. http://doi.org/10.1016/j.diin.2010.08.001

Citron, D. K. (2010). Fulfilling government 2.0's promise with robust privacy protections. *George Washington Law Review*. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-77955341233&partnerID=tZOtx3y1

Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties. *Analyses of Social Issues and Public Policy*, *5*(1), 263–276. http://doi.org/10.1111/j.1530-2415.2005.00071.x

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *JOURNAL OF GLOBAL INFORMATION MANAGEMENT*, *14*(4), 57–93. http://doi.org/10.4018/jgim.2006100103

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics*, *4*(4), 47–64. http://doi.org/10.1080/19331680801978759

Haikola, S., & Jonsson, S. (2007). State surveillance on the internet - The Swedish debate and the future role of libraries and LIS. *LIBRI*, *57*(4), 209–218. http://doi.org/10.1515/LIBR.2007.209

Irion, K. (2009). Privacy and securityInternational communications surveillance. *Communications of the ACM*, *52*(2), 26. http://doi.org/10.1145/1461928.1461940

Jiang, M., & Okamoto, K. (2014). National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike. *Policy & Internet*, *6*(1), 89–107. http://doi.org/10.1002/1944-2866.POI353

Kang, S., & Gearhart, S. (2010). E-Government and Civic Engagement: How is Citizens' Use of City Web Sites Related with Civic Involvement and Political Behaviors? *JOURNAL OF BROADCASTING & ELECTRONIC MEDIA*, *54*(3), 443–462. http://doi.org/10.1080/08838151.2010.498847

Keymolen, E., Prins, C., & Raab, C. (2012). Trust and ICT: New challenges for public administration. *Innovation and the Public Sector*, *19*, 21–35. http://doi.org/10.3233/978-1-61499-137-3-21

Krueger, B. S. (2005). Government surveillance and political participation on the Internet. *SOCIAL SCIENCE COMPUTER REVIEW*, *23*(4), 439–452. http://doi.org/10.1177/0894439305278871

Lips, M. (2010). Rethinking citizen-government relationships in the age of digital identity: Insights from research. *Information Polity*, *15*(4), 273–289. http://doi.org/10.3233/IP-2010-0216

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 129–141. http://doi.org/10.1016/j.giq.2015.01.003

Ventura, H. E., Miller, J. M., & Deflem, M. (2005). Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power. *Critical Criminology*, *13*(1), 55–70. http://doi.org/10.1007/s10612-004-6167-6

Wang, S. S., & Hong, J. (2010). Discourse behind the Forbidden Realm: Internet surveillance and its implications on China's blogosphere. *Telematics and Informatics*, *27*(1), 67–78. http://doi.org/10.1016/j.tele.2009.03.004

Xu, H., & Dinev, T. (2012). The security-liberty balance: individuals' attitudes towards internet government surveillance. *Electronic Government, an International Journal*, *9*(1), 46. http://doi.org/10.1504/EG.2012.044778

Generella teoretiska resonemang

21 artiklar

De artiklar som samlas under denna rubrik har det gemensamt att de inte först och främst presenterar egen empiri, utan främst för övergripande teoretiska diskussioner avseende framväxten av vad som av många benämns som övervakningssamhället. Då texterna i huvudsak bygger på sammanhängande resonmang över cirka 15 sidor, blir det svårt att på ett enkelt sätt sammanfatta innehållet här. Två återkommande begrepp är emellertid Pantopticon och Big Brother.

Den digitala teknikens stora möjligheter, för centrala aktörer, att följa enskildas beteenden beskrivs även i flera andra artiklar i termer av Pantopticon (Farinosi 2014; Ganascia 2010; Grodzinsky och Tavani 2005; Humphreys 2006; Kandias et al. 2014; Jiang och Okamoto 2014; Russett 2011). Det digitala samhället problematiseras här utifrån det faktum att det möjliggör massiv övervakning av samhällets alla medborgare. Men här beskrivs också hur de digitala strukturera kan användas av var och en och på så sätt stärka individens makt i förhållande till makten.

Ego-Panopticism: beskrivs som en ökad möjlighet för enskilda individer att, genom det digitala mediet, övervaka och sprida information avseende missförhållanden och maktmissbruk i samhället. Med andra ord ett omvänt panopticon, eller som de skriver **"**counter-panopticism". Panopticism syftar i detta fall tillbaka på Jeremy Benthams modell över det ideala fängelset där fången alltid (i vart fall potentiellt) är betraktad av övervakaren. "The individual is now an operative in the surveillance society so political and social elites are at risk of disclosure of aberrant behavior through instantaneous disclosure by any random witness. Accordingly, technology has created an evolution in societal power relationships." (Smith et al. 2011, s).

Big brother: Även Orwells dystopiska bild av det framtida övervakningssamhället som återfinns i romanen 1984 är flitigt refererad (Giroux 2015; Kang et al. 2012; Mordini och Rebera 2012; Stančin och Tomažič 2010; Van Otterlo 2014; Vitaliev 2007). I Zuboff 2015 används termern Big brother för att beskriva baksidorna med den flitiga handeln med och akumulation av potentiellt integritetskänslig personlig information. Då användardata samlas in i olika sammanhang för att sedan säljas vidare blir det följaktligen otydligt vem som har information om mig samt vilka konsekvenser detta kan medföra. Detta bekskrivs även i termer av Surveillance capitalism: "Surveillance capitalism offers a new regime of comprehensive facts and compliance with facts. It is, I have suggested, a *coup* from above – the installation of a new kind of sovereign power." (Zuboff 2015, s 86).

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*(1), 5–24. http://doi.org/10.1177/1367877909348536

Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, *6*(2), 119–134. http://doi.org/10.1177/1477370808100541

De Laat, P. B. (2008). Online diaries: Reflections on trust, privacy, and exhibitionism. *Ethics and Information Technology*, *10*(1), 57–69. http://doi.org/10.1007/s10676-008-9155-9

Earl, J. (2012). PRIVATE PROTEST? Public and private engagement online. *INFORMATION COMMUNICATION & SOCIETY*, *15*(4, SI), 591–608. http://doi.org/10.1080/1369118X.2012.665936

Ellis, D., Harper, D., & Tucker, I. (2013). The Dynamics of Impersonal Trust and Distrust in Surveillance Systems. *Sociological Research Online*, *18*(3). http://doi.org/10.5153/sro.3091

Farinosi, M. (2011). Deconstructing bentham's panopticon: The new metaphors of surveillance in the web 2.0 environment. *TripleC*, *9*(1), 62–76. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZOtx3y1

Ford, S. M. (2011). RECONCEPTUALIZING THE PUBLIC/PRIVATE DISTINCTION IN THE AGE OF INFORMATION TECHNOLOGY. *INFORMATION COMMUNICATION & SOCIETY*, *14*(4, SI), 550–567. http://doi.org/10.1080/1369118X.2011.562220

Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. *Sociology Compass*, *5*(2), 134–147. http://doi.org/10.1111/j.1751-9020.2010.00354.x

Fuchs, C. (2012). The Political Economy of Privacy on Facebook. *Television & New Media*, *13*(2), 139–159. http://doi.org/10.1177/1527476411415699

Giroux, H. A. (2015). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *CULTURAL STUDIES*, *29*(2), 108–140. http://doi.org/10.1080/09502386.2014.917118

Gurses, S., & Diaz, C. (2013). Two tales of privacy in online social networks. *IEEE Security & Privacy*, *11*(3), 29–37. http://doi.org/10.1109/MSP.2013.47

Humphreys, S. (2013). Predicting, securing and shaping the future: Mechanisms of governance in online social environments. *International Journal of Media & Cultural Politics*, *9*(3), 247–258. http://doi.org/10.1386/macp.9.3.247_1

Kang, J., Shilton, K., Estrin, D., Burke, J., & Hansen, M. (2012). Self-Surveillance Privacy. *IOWA LAW REVIEW*, *97*(3), 809–847. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84859056524&partnerID=tZOtx3y1

Kreissl, R. (2014). Assessing security technology's impact: old tools for new problems. *Science and Engineering Ethics*, *20*(3), 659–73. http://doi.org/10.1007/s11948-014-9529-9

Paliwala, A. (2013). Netizenship, security and freedom. *International Review of Law, Computers & Technology*, *27*(1-2), 104–123. http://doi.org/10.1080/13600869.2013.764139

Russett, P. C. (2011). A Contemporary Portrait of Information Privacy: Collective Communicative Consequences of Being Digital. *Review of Communication*, *11*(1), 39–50. http://doi.org/10.1080/15358593.2010.504882

Sevignani, S. (2012). The problem of privacy in capitalism and the alternative social networking site diaspora. *TripleC*, *10*(2), 600–617. Retrieved from

http://www.scopus.com/inward/record.url?eid=2-s2.0-84861721442&partnerID=tZOtx3y1

Shroff, M., & Fordham, A. (2010). «Do you know who i am?» Exploring identity and privacy. *Information Polity*, *15*(4), 299–307. http://doi.org/10.3233/IP-2010-0162

Smith, C. A., Bellier, T., & Altick, J. (2011). Ego-Panopticism: The Evolution of Individual Power. *New Political Science*, *33*(1), 45–58. http://doi.org/10.1080/07393148.2011.544477

Van Otterlo, M. (2014). Automated experimentation in walden 3.0: The next step in profiling, predicting, control and surveillance. *Surveillance and Society*, *12*(2), 255–272. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84901052294&partnerID=tZOtx3y1

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *JOURNAL OF INFORMATION TECHNOLOGY*, *30*(1), 75–89. http://doi.org/10.1057/jit.2015.5

Arbete

12 artiklar

På ett övergripande plan visar artiklarna att övervakning av anställdas förehavanden på Internet är tämligen vanligt förekommande. T ex redovisar Alder et al. (2008) att så många som 63 procent av de amerikanska företagen övervakar sina anställdas internetanvänding. Samtidigt lyfts flera potentiellt skadliga effekter fram såsom minskad tillit till arbetsgivaren, motivation och arbetstillfredsställelse. Dock är sambanden inte helt enkla, utan i vilken mån övervakningen har en negativ effekt på de anställda är beroende av hur rättfärdigad den bedöms samt ett antal andra faktorer såsom anställningstid exempelvis.

Ball (2010) sätter frågan om övervakning av anställda i ett historiskt perspektiv och argumenterar för att fenomenet i sig inte är något nytt utan funnits länge. Dock har den digitala tekniken möjliggjort mer långtgående och djupgående möjligheter att i detalj följa de anställdas beteende. Vidare argumenteras det för att denna typ av digital övervakning potentiellt har konsekvenser för såväl anställdas hälsa och välmående som motivation och kreativitet.

Alder et al. (2006; 2008) visar att övervakning av anställdas internetanvändning kan påverka tilliten till arbetsgivaren negativt, vilket i sin tur även får konsekvenser för arbetstillfredsställelse, engagemang och vilja att stanna i företaget. Framförallt när det sker utan att samtycke inhämtats eller att syfte klargjorts.

Även Samaranayake och Gamage (2012) studerar anställdas upplevelser av och attityder till att övervakas i det digitala på arbetsplatsen. Deras främsta slutats är att upplevelsen av att vara övervakad påverkade arbetstillfredsställelsen på ett negativt sätt. ”Perceived Invasion of Privacy is negatively correlated to job satisfaction. Software professionals, who were worried about their privacy being violated because of electronic monitoring, were rather dissatisfied in their job.” (Samaranayake och Gamage 2012, s 242).

Dock visar en fördjupad analys att detta samband försvagas desto längre anställningstid de anställda hade. ”According to the regression model outputs developed based on the professional experience of the software professionals, the variation in job satisfaction explained by the independent variables decreased with higher professional experience. Also none of the variables were significant for the regression models developed for the groups of 10–15 years of experience and above 15 years of experience. This implies that the impact of electronic monitoring towards the job satisfaction becomes less significant with the maturity of the software professionals.” (Samaranayake och Gamage 2012, s 243). Samtidigt argumenteras det för att negativa upplevelser av övervakning kan förebyggas med information och tydliga policys. ”It is important that a policy for electronic monitoring exists at the

first place, and is communicated to all employees properly. This would effectively reduce the negative impacts of electronic monitoring associated with job satisfaction of the software professionals in Sri Lanka." (Samaranayake och Gamage 2012 s 243). Ett resonemang som ligger väl i linje med Adler et al. (2006).

Wen och Gershuny (2005) diskuterar de legala aspekterna av digital övervakning av anställda. På samma sätt som övriga artiklar som behandlar legala aspekter av övervakning och integritet i det digitala pekar de rättens svårighet att hänga med i den tekniska utvecklingen vilket innebär att skyddet för den enskilde anställde är svagt. I de fall ett ärende nått till rättegången har utfallet nästan alltid varit till arbetsgivarens favör. "Court decisions have supported employer monitoring of employees' email. Courts have even allowed the use of video cameras in employee changing rooms when the employer's objective was to prevent theft. Despite these favorable decisions, workplace privacy law in America is still in its infancy and gaps exist between the capability of the employer to monitor and the factual scenarios of the cases brought to court. For example, although monitoring employee website visits is a common practice, only a few cases have currently challenged its legitimacy" (Wen och Gershuny 2005, s 169). Avslutningsvis i artikeln argumenteras för vikten av att företagen utvecklar policys inom området. "companies need to develop computer-based monitoring policies for employees who have access to the Internet. It is also important to keep monitoring in perspective – it should not replace critical managerial skills and behaviors needed in the workplace." (Wen och Gershuny 2005, s 173).

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *INFORMATION & MANAGEMENT*, *43*(7), 894–903. http://doi.org/10.1016/j.im.2006.08.008

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *JOURNAL OF BUSINESS ETHICS*, *80*(3), 481–498. http://doi.org/10.1007/s10551-007-9432-2

Arlitt, M., Carlsson, N., Gill, P., Mahanti, A., & Williamson, C. (2011). Characterizing Intelligence Gathering and Control on an Edge Network. *ACM TRANSACTIONS ON INTERNET TECHNOLOGY*, *11*(1). http://doi.org/10.1145/1993083.1993085

Ball, K. (2010). Workplace surveillance: an overview. *LABOR HISTORY*, *51*(1), 87–106. http://doi.org/10.1080/00236561003654776

Chen, J. V., Chen, C. C., & Yang, H.-H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *INDUSTRIAL MANAGEMENT & DATA SYSTEMS*, *108*(1-2), 87–106. http://doi.org/10.1108/02635570810844106

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. (2009). Effects of electronic mail policies on invasiveness and fairness. *JOURNAL OF MANAGERIAL PSYCHOLOGY*, *24*(6), 502–525. http://doi.org/10.1108/02683940910974107

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *TELEMATICS AND INFORMATICS*, *29*(2), 233–244. http://doi.org/10.1016/j.tele.2011.08.003

Searle, R. H. (2006). New technology: the potential impact of surveillance techniques in recruitment practices. *PERSONNEL REVIEW*, *35*(3), 336–351. http://doi.org/10.1108/00483480610656720

Van Gramberg, B., Teicher, J., & O'Rourke, A. (2014). Managing electronic communications: a new challenge for human resource managers. *INTERNATIONAL JOURNAL OF HUMAN RESOURCE MANAGEMENT*, *25*(16), 2234–2252. http://doi.org/10.1080/09585192.2013.872166

Wen, H. J., & Gershuny, P. (2005). Computer-based monitoring in the American workplace: Surveillance technologies and legal challenges. *Human Systems Management*. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-22344442448&partnerID=tZOtx3y1

Wen, H. J., Schwieger, D., & Gershuny, P. (2007). Internet usage monitoring in the workplace: Its legal challenges and implementation strategies. *INFORMATION SYSTEMS MANAGEMENT*, *24*(2), 185–196. http://doi.org/10.1080/10580530701221072

Whitty, M. T., & Carr, A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behaviour in the workplace. *COMPUTERS IN HUMAN BEHAVIOR*, *22*(2), 235–250. http://doi.org/10.1016/j.chb.2004.06.005

Kunskap och beteende bland unga

17 artiklar

Detta forskningsfält behandlar frågan om attityder till integritet på Internet (”Privacy perception/concerns”) relaterat till främst utbildning. I relation till detta diskuteras även frågor om socio-ekonomisk klasstillhörighet och skillnader i kunskapsnivåer (”Digital/privacy literacy”) samt olika pedagogiska grepp för att stärka individers kunskaper om Internet samt möjliggöra ett mer utvecklat säkerhetstänkande kring hur information hanteras i det digitala. Eller som Park (2013a, s. 3) uttrycker det: ” In short, to exercise appropriate measures of resistance against the potential abuse of personal data, it may be that users should be able to understand data flow in cyberspace and its acceptable limits of exposure” Park (2013b) pekar på stora skillnader i kunskapsnivåer och insikter i integritetsfrågor av internetanvändare vilka kan härledas till socio-ekonomisk status. I detta sammanhang uppmanas till särskilda riktade insatser mot utsatta grupper i syfte att jämna ut klasskillnader: ”Dissemination of personal information skill and knowledge is a salient issue in marginalized communities, as lacking the power to understand and resist surveillance can have negative consequences such as potential discrimination in one’s digital engagement.”(Park 2013b, s. 698).

Oulasvirta et al. (2014) visar att upplevd oro i förhållande till integritet i det digitala ökar när användare övervakas/kartläggs utan att avsändare och syfte är tydligt. Forskningsrojektet beskrivs enligt följande: ”An online experiment (n = 1,897) was carried out to understand how data disclosure practices in ubiquitous surveillance affect users’ privacy concerns. Information about the identity and intentions of a data collector was manipulated in hypothetical surveillance scenarios. Privacy concerns were found to differ across the scenarios and moderated by knowledge about the collector’s identity and intentions. Knowledge about intentions ex- hibited a stronger effect. When no information about intentions was disclosed, the respondents postulated negative intentions. A positive effect was found for disclosing neutral intentions of an organization or unknown data collector, but not for a private data collector. The findings underline the importance of disclosing intentions of data use to users in an easily understandable manner.” (Oulasvirta et al. 2014, s. 1). Följdaktligen gäller att transperans på ett signifikant sätt minskar förekomsten av oro. Utifrån detta konkluderas att: “The present findings underline that both the data collector’s identity and intention should be disclosed in such privacy nutrition labels. Furthermore, while exposing the two factors (identity and intention) will be beneficial, directing the user’s attention to the data collector’s intention will have a stronger effect than would drawing attention to identity alone.” (Oulasvirta et al. 2014, s. 5).

Berger et al. (2014) visar att ungdomars upplevelser av att vara övervakad på Internet kan leda till minskad nätanvändning: ”The findings indicate a significant quantitative decrease in Internet activity of users believing to be monitored.” (Berger et al. 2014).

Utbildning inom området behandlas i termer av ”E-safety education” och beskrivs på följande sätt: “E-safety refers to the way young people are taught about risks online, how they can protect themselves and to whom they should report worrying activity. Education is understood as one of a range of explicit strategies enacted by actors in the politics of digitally mediated surveillance.” (Barnard-Wills 2012, s. 240). Bakgrunden till behovet av riktade utbildningar kring E-safety riktat mot unga människor motiveras av gruppens särskilt utsatta ställning som såväl offer som gärninspersoner: Children are a population who are constructed as both potential victims and potential offenders in online settings. They are at risk from exposure to inappropriate media and from hostile actors. However they seek to circumvent restrictions on their behaviour, and can be responsible for harmful behaviour to each other in the form of cyber-bullying.” (Barnard-Wills 2012, s 248). Steeves och Regan (2014, s 299) beskriver ett antal olika initiativ till webbutbildningar riktade mot unga Internetanvändare: ”Educational programs typically reinforce this approach to privacy as informational control. For example, the European Union’s Ins@fe initiative, the myprivacy.mychoice.mylife (2013) campaign created by the Privacy Commissioner of Canada (2008) and the US government’s Kids.gov (2013) site all itemize the dangers associated with disclosing personal information online and encourage young people to limit what they say about themselves in online spaces. These sites advise young people that disclosing information opens them up predation and bullying; they link privacy – again defined as the non-disclosure of personal information – directly to safety.” Isasi-Andrieu et al. (2012) beskriver verktyget ”Gazela” vilket är avsett att hjälpa unga spanska Internetanvändare att bättre värdera och hantera intergritetsfrågor online.

Amos, C., Zhang, L., & Pentina, I. (2014). Investigating Privacy Perception and Behavior on Weibo. *JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING*, *26*(4), 43–56. http://doi.org/10.4018/joeuc.2014100103

Barnard-Wills, D. (2012). E-safety education: Young people, surveillance and responsibility. *CRIMINOLOGY & CRIMINAL JUSTICE*, *12*(3), 239–255. http://doi.org/10.1177/1748895811432957

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Isasi-Andrieu, A., Lopez-Carrera, A., & Ruiz-Ibanez, P. (2012). Gazela: social networks’ digital advisor for teenagers. *PROFESIONAL DE LA INFORMACION*, *21*(5), 514–519. http://doi.org/10.3145/epi.2012.sep.11

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.)*Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-662-44788-8

Netchitailova, E. (2012). Facebook as a surveillance tool: From the perspective of the user. *TripleC*, *10*(2), 683–691. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84871454614&partnerID=tZOtx3y1

Orman, H. (2015). Why Won't Johnny Encrypt? *IEEE Internet Computing*, *19*(1), 90–94. http://doi.org/10.1109/MIC.2015.16

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 633–8. http://doi.org/10.1089/cyber.2013.0585

Park, Y. J. (2013a). Digital Literacy and Privacy Behavior Online. *COMMUNICATION RESEARCH*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J. (2013b). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *SOCIAL SCIENCE COMPUTER REVIEW*, *31*(6), 680–702. http://doi.org/10.1177/0894439313485202

Park, Y. J., Jang, S. M., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

Ross, J. (2011). Traces of self: online reflective practices and performances in higher education. *TEACHING IN HIGHER EDUCATION*, *16*(1), 113–126. http://doi.org/10.1080/13562517.2011.530753

Stančin, S., & Tomažič, S. (2010). User created content privacy or big brother is watching you. *Elektrotehniski Vestnik/Electrotechnical Review*, *77*(1), 5–12. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-77957199564&partnerID=tZOtx3y1

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. http://doi.org/10.1108/JICES-01-2014-0004

Vickery, J. R. (2015). `I don't have anything to hide, but horizontal ellipsis `: the challenges and negotiations of social and mobile media privacy for non-dominant youth. *INFORMATION COMMUNICATION & SOCIETY*, *18*(3, SI), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Hälsa

14 artiklar

En stor del av artiklarna inom detta område berör integritetsaspekter i relation till den ökade möjligheten att genom att följa nätanvändares digitala spår förutspå och intervenera för att stoppa smittspridning. Detta kan t.ex. ske genom verktyget ”Google trends”. Nuti et al. (2014) beskriver detta verktyg och dess potential på följande sätt: ”Google Trends analyzes a portion of the three billion daily Google Search searches and provides data on geospatial and temporal patterns in search volumes for user-specified terms. […]Google Trends holds potential as a free, easily accessible means to access large population search data to derive meaningful insights about population behavior and its link to health and health care.” (Nuti et al. 2014, s. 1 ff). Studien visar att Google trends står sig väl i relation till andra sätt att uppskatta och kartlägga hälsa och hälsobeteende. Trots möjligheterna som finns inbyggda i verktyget återstår dock arbete med utveckling: ”Google Trends could have been used to forecast the peak of scarlet fever in the UK 5 weeks before its arrival. Although studies are promising, strong correlations alone do not support the use of Google Trends for surveillance, and further work is needed to substantiate the reliability and real world applicability of Google Trends as a tool to monitor health-related phenomena.” (Nuti et al. 2014, s. 46). I relation till detta visar Gunn och Lester (2013) att sökningar på självmord kan vara ett bra sätt att på ett tidigt stadium fånga upp problemet och genomföra interventioner. Även Gu et al. (2014) visar att analyser av Internetsökningar kan vara ett bra sätt att tidigt kunna sätta in insatser vid epedemier. Cooper et al. (2005) argumenterar dock att det inte enbart är sjukdomsfallen i sig som genererar sökningar på Internet. I artikeln som behandlar cancer argumenterar de för att även mediaexponering av vissa sjukdomstillstånd tenderar att generera sökningar.

Gemensamt för de artiklar som behandlar möjligheterna att utifrån indivders digitala fotspår, i termer av sökningar (Cooper et al. 2005; Gunn och Lester 2013; Nuti et al. 2014;), blogginlägg (Gu et al. 2014), twitterflöden (Velardi et al. 2014), Facebooklikes (Gittelman et al. 2015) eller eget program som tankade ner information från flera olika källor på Internet (D’Ambrosio et al. 2015) är att de (förvånansvärt nog) överhuvudtaget inte behandlar integritetsfrågan alls utan enbart ser möjligheter med den digitala utvecklingen. Anledningen till att de kommit med i sökningen och gallringen är att begreppet ”Surveillance” förkommer flitigt. Men då enbart med innebörden: att genom insamling av data skaffa sig en god bild över ett fenomen.

Integritetsfrågan förekommer däremot tydligare när diskussionen rör digitalisering av den reguljära vården, vad gäller t ex elektronisk lagring och hantering av känslig personlig information. T ex skriver Kramer et al. (2012 , s. 7): ”The rapid proliferation of medical devices, and their growing sophistication, presents Internet-age challenges for multiple stakeholders. Without an understanding of security and privacy, it will be difficult for patients and clinicians to establish confidence in device safety and effectiveness.”

Även inom området e-hälsa (m-health eller e-health) finns en diskussion kring hanteringen av potentiellt integritetskänslig information (Lupton 2012; Lupton 2015). Särskilt då i relation data som genereras genom olika hälsoappar där användaren själv frivilligt mäter motionsvanor och anger andra typer av hälsobeteende som kost t.ex. Framförallt för Lupton resonemang kring hur fenomenet (att ständigt vara mätt och bedömd) påverkar vår självbild:

"Will the 'nagging voices' of the health-promoting messages automatically issuing forth from a person's mobile device be eventually ignored by its user? Or will these messages incite even greater feelings of guilt and shame at one's lack of self-control and self-discipline? Alternatively, will m-health technologies produce a cyborg, post-human self in which the routine collection of data about bodily actions and functions is simply incorporated unproblematically into the user's sense of selfhood and embodiment? How will concepts of 'health' itself be shaped and understood in a context in which one's biometric indicators may be constantly measured, analysed and displayed publicly on Facebook or Twitter? Will the 'objective' measurements offered by mobile devices take precedence over the 'subjective' assessments offered by the senses of the fleshly body?" (Lupton (2012, s. 242)

Boulos, M. N. K., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *BIOMEDICAL ENGINEERING ONLINE*, *10*. http://doi.org/10.1186/1475-925X-10-24

Cooper, C. P., Mallon, K. P., Leadbetter, S., Pollack, L. A., & Peipins, L. A. (2005). Cancer Internet search activity on a major search engine, United States 2001-2003. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *7*(3). http://doi.org/10.2196/jmir.7.3.e36

Curtis, B. L. (2014). SOCIAL NETWORKING AND ONLINE RECRUITING FOR HIV RESEARCH: ETHICAL CHALLENGES. *JOURNAL OF EMPIRICAL RESEARCH ON HUMAN RESEARCH ETHICS*, *9*(1), 58–70. http://doi.org/10.1525/jer.2014.9.1.58

D'Ambrosio, A., Agricola, E., Russo, L., Gesualdo, F., Pandolfi, E., Bortolus, R., … Tozzi, A. E. (2015). Web-Based Surveillance of Public Information Needs for Informing Preconception Interventions. *PLOS ONE*, *10*(4). http://doi.org/10.1371/journal.pone.0122551

Davies, S. E. (2012). Nowhere to hide: informal disease surveillance networks tracing state behaviour. *Global Change, Peace & Security*, *24*(1), 95–107. http://doi.org/10.1080/14781158.2012.641272

Gittelman, S., Lange, V., Crawford, C. A. G., Okoro, C. A., Lieb, E., Dhingra, S. S., & Trimarchi, E. (2015). A New Source of Data for Public Health Surveillance: Facebook Likes. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *17*(4). http://doi.org/10.2196/jmir.3970

Gu, H. y, Chen, B., Zhu, H., Jiang, T., Wang, X., Chen, L., … Jiang, J. (2014). Importance of Internet Surveillance in Public Health Emergency Control and Prevention: Evidence From a Digital Epidemiologic Study During Avian Influenza A H7N9 Outbreaks. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *16*(1). http://doi.org/10.2196/jmir.2911

Gunn, J. F., & Lester, D. (2013). Using google searches on the internet to monitor suicidal behavior. *Journal of Affective Disorders*, *148*(2-3), 411–2. http://doi.org/10.1016/j.jad.2012.11.004

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE*, *7*(7). http://doi.org/10.1371/journal.pone.0040200

Lupton, D. (2012). M-health and health promotion: The digital cyborg and surveillance society. *SOCIAL THEORY & HEALTH*, *10*(3), 229–244. http://doi.org/10.1057/sth.2012.6

Lupton, D. (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–53. http://doi.org/10.1080/13691058.2014.920528

Myers, J., Frieden, T. R., Bherwani, K. M., & Henning, K. J. (2008). Privacy and public health at risk: Public health confidentiality in the digital age. *AMERICAN JOURNAL OF PUBLIC HEALTH*, *98*(5), 793–801. http://doi.org/10.2105/AJPH.2006.107706

Nuti, S. V, Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The Use of Google Trends in Health Care Research: A Systematic Review. *PLOS ONE*, *9*(10). http://doi.org/10.1371/journal.pone.0109583

Velardi, P., Stilo, G., Tozzi, A. E., & Gesualdo, F. (2014). Twitter mining for fine-grained syndromic surveillance. *Artificial Intelligence in Medicine*, *61*(3), 153–63. http://doi.org/10.1016/j.artmed.2014.01.002

Handel

12 artiklar

I centrum för artiklarna inom området handel är studiet av relationen mellan attityder till övervakning (privacy concerns) relaterat till köpbeteende (consumer behaviour) (Park et al. 2012; Park 2014). Resultaten mellan studierna spretar lite grand. T ex undersöker Park et al. (2012) huruvida oro för att integritetskänslig information skulle hamna i fel händer påverkar konsumenters beteende på Internet och kommer fram till: ”concern did not play a meaningful role in predicting the social dimension of privacy protection, such as avoiding certain web sites or falsifying information to hide one’s identity.” (Park et al. 2012, s. 1023-1024). Detta ligge i linje med Park (2014) som studerat huruvida det spelar någon roll i vilken mån en kommersiell hemsida tar hänsyn till hur integritetskänslig information hanteras i förhållande till antalet besökare till sidan. Med hanteringen av integritetskänslig information avses i detta fall om besökaren på hemsidan har möjlighet att styra vilken information denne delar med sig av. The central question is whether and to what extent the website interface is constructed as an enabler for informed choice in managing personal information. Here information privacy is defined as the ability to control one’s personal data and associated identities; widely regarded as one of the most vulnerable aspects of online use.” (Park 2014, s. 360-361). Som följande titel antyder, *A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites*, kan man inte förlita sig på att hänsynen till den personliga integriteten bland kommersiella aktörer ska öka genom att potentiella kunder väljer bort de aktörer som brister i detta hänseende. Detta då forskningen visar att möjligheten att påverka nivån på ”information privacy” inte spelar någon roll för konsumentbeteendet online. Forskningen beskrivs på följande sätt: ”This article examines user control of privacy online as indicated by functional features of commercial websites. While prior studies have focused on what’s written in privacy policy statements, systematic attention on the interactive aspects of the Web have been scant. This analysis, based on a sample of 398 commercial sites in the United States, shows that the more popular sites did not necessarily provide better privacy control features for users than sites that were randomly selected. In addition, there was no clear relationship between website characteristics and the functional features of privacy control.” (Park 2014, s. 360).

I oppossition till ovan hävdar Mercovic (2010) att frågor om hur integritet och hur personlig information hanteras visst spelar roll för konsumentbeteende och att företag som inte uppmärksammar detta faktum riskerar att förlora kunder. Dock formas, enligt artikelförfattaren, inte dessa uppfattningar så mycket av säkerhetsintställningar på enskilda hemsidor (som Park 2014 studerat ovan) utan snarare av organisationen bakom hemsidan.

I syfte att kunna förstå konsumenters vilja respektive ovilja att dela med sig av personlig information på Internet argumentera Li (2012)och Mekovic (2010) att vi måsta ta hänsyn till upplevd nytta med att göra så i relation till risk. Med andra ord handlar beslutet i slutändan inte enbart om tillit till organisationen eller en enskild hemsidas design och funktion; utan för att förstå konsumenters beteende online måste det vägas in upplevd nytta med att delge

personlig information. Li (2012) beskriver denna beräkning i termer av *calculus* (i.e., the trade-off between expected benefits and privacy risks).

Draper (2012) vänder sig mot bilden av att det är ”kundens inflytande/makt” som står i fokus vid datainsamling, eftersom kundens makt likställt med vad man beskriver som kundnytta. Kundnyttan beskrivs enligt följande: “…give you a more enjoyable, convenient shopping experience and to help us identify and/or provide information, products or services that may be of interest to you. The suggestion that personal data is used to help create a more relevant user experience may refer to the deals offered, the website content or the advertisements served.” (Draper 2012, s. 403). Istället handlar det om den ökade möjligheten att formulera riktade erbjudanden till kunder:” With the information these companies have about users, the ability to offer deals that are targeted based on an individual’s online reputation or profile (accurate or not) is immense.” (Draper 2012, s. 404). Och avslutar med: There is reason to be concerned about a business model that promotes the power of the consumer while simultaneously using information about that individual to create a unique consumer experience, the basis for which is beyond their control.” (Draper 2012, s. 405). Det som av företagen beskrivs som “kundens makt” handlar i praktiken om att skräddarsy reklam i syfte att maximera försäljning.

Draper, N. A. (2012). Group power: Discourses of consumer power and surveillance in group buying websites. *Surveillance and Society*, *9*(4), 394–407. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84873520765&partnerID=tZOtx3y1

Ghani, N. A., & Sidek, Z. M. (2009). Personal information privacy protection in e-commerce. *WSEAS Transactions on Information Science and Applications*, *6*(3), 407–416. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-66349109339&partnerID=tZOtx3y1

Humphreys, A. (2006). The Consumer as Foucauldian “Object of Knowledge.” *Social Science Computer Review*, *24*(3), 296–309. http://doi.org/10.1177/0894439306287975

Katos, V. (2012). An integrated model for online transactions: illuminating the black box. *Information Management & Computer Security*, *20*(3), 184–206. http://doi.org/10.1108/09685221211247299

L. Finn, R., & Wadhwa, K. (2014). The ethics of “smart” advertising and regulatory initiatives in the consumer intelligence industry. *Info*, *16*(3), 22–39. http://doi.org/10.1108/info-12-2013-0059

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *DECISION SUPPORT SYSTEMS*, *54*(1), 471–481. http://doi.org/10.1016/j.dss.2012.06.010

Mekovec, R. (2010). Online privacy: Overview and preliminary research. *Journal of Information and Organizational Sciences*. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-79960110760&partnerID=tZOtx3y1

Michael, M. G., Michael, K., & Perakslis, C. (2015). Überveillance, the web of things, and people: What is the culmination of all this surveillance? *IEEE Consumer Electronics Magazine*, *4*(2), 107–113. http://doi.org/10.1109/MCE.2015.2393007

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of `datification'. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *24*(1), 3–14. http://doi.org/10.1016/j.jsis.2015.02.001

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy & Internet*, *6*(4), 360–376. http://doi.org/10.1002/1944-2866.POI375

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027. http://doi.org/10.1016/j.chb.2012.01.004

Winter, J. S. (2014). Surveillance in ubiquitous network societies: normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. *ETHICS AND INFORMATION TECHNOLOGY*, *16*(1), 27–41. http://doi.org/10.1007/s10676-013-9332-3

Privata relationer

9 artiklar

Den digitala tekniken har inte enbart erbjudit ökade möjligheter för företag och stater att övervaka invidier. Detta sker även i enskilda privata relationer. Fokus här ligger framförallt på den möjighet att följa en partners eller före detta partners förehavanden på sociala medier. Det rör sig med andra ord inte om någon form av illegal verksamhet utan om en möjlighet att följa en annan persons digitala fotspår på Internet. Helsper och Whitty (2010) visar att det är tämligen vanligt att övervaka en (ex)partners digitala fotspår, såsom SMS, e-post och internethistorik: ”The findings show that there are surprisingly high levels of surveillance but that the types of surveillance used are quite limited. In around a third of the couples at least one person checked their partner’s emails or read their partner’s SMS messages without them knowing and in a fifth of the couples at least one of the partners had checked their spouse’s browser history.” (Helsper och Whitty 2010, s. 924).

Marshall (2012) har studerat hur tidigare partners hanterar sina relationer på Facebook post preakup, d.v.s. efter det att relatioen avslutats, samt vilka konsekvenser detta kan få för hälsa och välmående. Resultaten tyder på att de som vidhåller en vänskap på Facebook efter det att relationen avbrutits kan hindras i sin personliga mognad och förmåga att gå vidare i livet. Samtidigt uttrycker denna grupp, lite överaskande flera positiva aspketer: ”Contrary to expectations, people who remained Facebook friends with an ex-partner were lower in negative feelings, sexual desire, and longing for the former partner than people who were not Facebook friends.” (2012, s. 523). Detta i relation till Lukacs och Quan-Haase (2015) som mer entydigt visar att de som ägnar sig åt intesiv efterforskning av tidigare partners förehavanden på Facebook överlag upplever en högre grad av emotionellt lidande.

Även Tong (2013) har studerat övervakning av tidigare partners via Facebook och då med fokus på vilken information som eftersöks. Föga överaskande handlar det om sociala relationer, förekomsten av en eventuell ny partner, samt olika åsikter om den tidigare relationen. Samtidigt framkommer det tydligt att sociala normer avseende denna typ av övervakning spelar en viktigt roll: ”The correlationally based analyses indicate that the more the individuals apprehend the social disapproval associated with ex-partner surveillance, the less they engage in the behavior. They either interact directly with the ex-partner (a focus that was not deterred by concerns over network approval), or do not inquire at all. Or, individuals who care less about what others’ think may be using Facebook more than those who are concerned with social approval.” (Tong 2013, s. 792).

Denna typ av passiv insamling av data, som en tidigare partner frivilligt lämnar i sociala medier, drabbar som sagt mest den som själv samlar in datan. Dock finns fall där övervakningen gått längre och mer kommit att likna stalking. Chaulk och Jone (2011) beskriver flera olika sätt genom vilket Facebook kan användas i detta ändamål. T ex kan ex-partnerns

statusuppdateringar avslöja var denne kommer att befinna sig vid en viss tidpunkt: ”We find that offenders use Facebook to facilitate primary contact by providing information about where a target might be (e.g., at specific events advertised on Facebook, or showing up at locations mentioned by the target in their profile).” Det kan även röra sig om att skicka upprepade meddelanden till ex-partnern eller dennes vänner och familj, skicka virtuella presenter och inbjudningar eller skriva inlägg på ex-partnerns Facebook-sida. Även Grattagliano et al. (2012) skriver om stalking i det digitala och delar in beteendet i tre nivår där den tredje omfattar direkta hot: ”1) following (including showing up at the victim's home and workplace, maintaining surveillance, and setting up coincidences); 2) communicating (by telephone, mail, leaving notes, graffiti, gifts, e-mail, and internet); including the ordering of goods and services in the victim's name; 3) attacking or committing acts of violence (threats, direct harassment of the victim or of people close to the victim, damaging of personal goods, false accusations, physical or sexual violence).” (Grattagliano et al. 2012, s. 65).

Chaulk, K., & Jones, T. (2011). Online Obsessive Relational Intrusion: Further Concerns About Facebook. *Journal of Family Violence*, *26*(4), 245–254. http://doi.org/10.1007/s10896-011-9360-x

Fox, J., & Warber, K. M. (2014). Social Networking Sites in Romantic Relationships: Attachment, Uncertainty, and Partner Surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3–7. http://doi.org/10.1089/cyber.2012.0667

Grattagliano, I., Cassibba, R., Greco, R., Laudisa, A., Torres, A., & Mastromarino, A. (2012). Stalking: old behaviour new crime. Reflections on 11 cases assessed in the judicial district of Bari. *RIVISTA DI PSICHIATRIA*, *47*(1), 65–72.

Gregg, M. (2013). Spousebusting: Intimacy, adultery, and surveillance technology. *Surveillance and Society*, *11*(3), 301–310. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84889685033&partnerID=tZOtx3y1

Helsper, E. J., & Whitty, M. T. (2010). Netiquette within married couples: Agreement about acceptable online behavior and surveillance between partners. *COMPUTERS IN HUMAN BEHAVIOR*, *26*(5), 916–926. http://doi.org/10.1016/j.chb.2010.02.006

Lukacs, V., & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. *INFORMATION COMMUNICATION & SOCIETY*, *18*(5, SI), 492–508. http://doi.org/10.1080/1369118X.2015.1008540

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior and Social Networking*, *15*(10), 521–6. http://doi.org/10.1089/cyber.2012.0125

McEwan, B. (2013). Sharing, caring, and surveilling: an actor-partner interdependence model examination of Facebook relational maintenance strategies. *Cyberpsychology, Behavior and Social Networking*, *16*(12), 863–9. http://doi.org/10.1089/cyber.2012.0717

Tong, S. T. (2013). Facebook use during relationship termination: uncertainty reduction and surveillance. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 788–93. http://doi.org/10.1089/cyber.2012.0549

Mänskliga rättigheter i det digitala

4 artiklar

Den gemensamma problemställningen för dessa artiklar är relationen mellan å ena sidan enskilda staters behov och önksemål att förebygga hot mot medborgarana och å andra sidan problemet med att grundläggande mänskliga rättigheter åsidosätts när jakten på t.ex. terrorister hamnar i förgrunden. Självklart har denna problemställning en bakgrund i ”September 11” och den rättsliga reaktionen från Bushadminstrationen ”the USA Patriot act” som bland annat gav den amerikanska staten ett utökat mandat att övervaka individers kommunikation. McAdams(2005) formulerar spänningen mellan risk, säkerhet och grundläggande mänskliga rättigheter i en fråga: ”is the nature of the threat from transnational terrorism so great that it could permanently shift the balance between personal privacy and national security in the direction of the latter priority?” (McAdams 2005, s 480). I samma artikel konkluderas dock att oron kan vara obefogad: ”In short, there has not been a straightforward, causal relationship between the U.S. campaign against terrorism and the limitation of Fourth Amendment rights.” (McAdams 2005, s. 495).

Även O´Brien (2014) adresserar området risk, säkerhet och mänskliga rättigheter med fokus på den Australiensiska kontexten och hur barnens rättigheter tas tillvara. Ett problem som nämns här att risken (för tillexempel groming) övervärderas och att barnens egen förmåga att ta ställning till risker och hantera dessa undervärderas: ”Foremost amongst these is that welfare discourse homogenises children as passive victims, entirely lacking the skills to refuse advances from online predators. Contradicting this conception is the emerging body of evidence indicating that Australian children demonstrate discretion and significant critical literacy in negotiating online risks. Indeed, of the children who choose not to use social networking sites 23% chose not to do so because of concerns about cyber-safety.” (O´Brien 2014, s. 755-756). I relation till detta uppmanar författaren till att i större utsträckning se barn och unga som aktiva individer och inte som passiva objekt vars röster måste lyssnas till: ”Policy makers, legislators and educators must acknowledge the importance in balancing children’s rights to protection *and* autonomy. For children’s rights to be fully respected this balance *must* be relative to the evolving capacities of the child, and children *must* have the opportunity to contribute their voices to the policy agendas that will greatly effect them.” (O´Brien 2014, s. 771).

Hiranandani (2011) argumenterar för att terrorbegreppet är för inkludernade och missbrukas för att rättfärdiga långgående intrång i den personliga integriteten. I artikeln manas till ett ökat fokus på vikten att ta hänsyn till personlig integritet som en grundläggande mänsklig rättighet: ”The post-9/11 trend seems to be towards capitalising on fear while playing down the intrusive nature and repressive potential of surveillance and information technologies.97 Public awareness is key to create a shift in opinions about the potentially dangerous effects of new technologies given the lack of adequate protections to prevent their abuse. The power lies in public outcry and legislative/parliamentary action to demand transparency and accountability on part of the watchers.” (Hiranandani 2011, 1102).

Hankey, S., & O Clunaigh, D. (2013). Rethinking Risk and Security of Human Rights Defenders in the Digital Age. *Journal of Human Rights Practice*, *5*(3), 535–547. http://doi.org/10.1093/jhuman/hut023

McAdams, A. J. (2005). Internet surveillance after September 11 - Is the United States becoming Great Britain? *COMPARATIVE POLITICS*, *37*(4), 479+.

O'Brien, W. (2014). Australia's Digital Policy Agenda. *The International Journal of Children's Rights*, *22*(4), 748–775. http://doi.org/10.1163/15718182-02204004

Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights*, *15*(7), 1091–1106. http://doi.org/10.1080/13642987.2010.493360

Sousveillance

3 artiklar

Ett intressant begrepp i sammanhanget är ”Sousveillance” vilket kan beskrivas som en reaktion på den ökade övervakningen av individer från stater och företag. Begreppet kan knytas till begreppet Ego-Panopticism som diskuterades i avsnittet om generella teoretiska resonemang ovan. Grundtanken med Sousveillance är att vända på kikaren så att övervakaren blir den övervakade. Här skapar övervakning och intrång i den personliga integriteten en reaktion och nya beteenden vilka tar sig yttryck i att medborgare med hjälp av digital teknik utsätter makthavare för övervakning. Fernback (2013, s. 11) beskriver det som ”Sousveillance is "watching from below," a form of inverse surveillance in which people monitor the surveillors. Examples include citizen video, watchdog web sites, or the monitoring of authorities (corporations, military, government). Sousveillance embraces the idea of transparency as an antidote to concentrated power in the hands of surveillors.” Exempel på medel och forum som kan användas i detta syfte är diskussionsgrupper på Facebook (intressant nog mest riktade mot forumet som används. T ex gruppen *Petition: Facebook, Stop Invading My Privacy*) (Fernback 2013), digitalt samordnad produktion och spridning av videofilmer av polisövervåld (Bradshaw (2013) och spridning av, för polisen kompromenterande, övervakningsfilmer som ljudfiler (Ganascia 2010).

Förhoppningar och utmaningar inför framtiden: ”While the potential remains for sousveillance to assist global justice activists in challenging authority and seeking alternative solutions to neoliberal globalization, an emancipatory relationship to social media and digital communication technologies is something that is not given, but must be critically and continuously forged. (Braadshaw 2013, s. 410)

Bradshaw, E. A. (2013). This is What a Police State Looks Like: Sousveillance, Direct Action and the Anti-corporate Globalization Movement. *CRITICAL CRIMINOLOGY*, *21*(4), 447–461. http://doi.org/10.1007/s10612-013-9205-4

Fernback, J. (2013). Sousveillance: Communities of resistance to the surveillance environment. *Telematics and Informatics*, *30*(1), 11–21. http://doi.org/10.1016/j.tele.2012.03.003

Ganascia, J.-G. (2010). The generalized sousveillance society. *Social Science Information*, *49*(3), 489–507. http://doi.org/10.1177/0539018410371027

Övrigt

5 artiklar

Här rymms artiklar som inte riktigt passade in under någon annan kategori. Bland annat en artikel som introducerar begreppet ”Cyber-Paranoia” vilket beskriver ett tillstånd av obefogad skräck för hot på Internet hos individer (Mason et al. 2014).

Garnar (2012) behandlar frågan med missbruk av offentliga datorer och därmed behovet av att begränsa och övervaka användningen.

Park et al. (2015) beskriver ett antal personlighetstyper relaterat till konsumentbeteende på Internet.

Lin och Lo (20105) beskriver ett nytt sätt för datainsamling av trafikdata på motorvägar och potentiella integritetsfrågor i relation till detta.

Andrejevic, M. (2007). Ubiquitous computing and the digital enclosure movement. *MEDIA INTERNATIONAL AUSTRALIA*, (125), 106–117.

Garnar, M. L. (2012). For the Sake of One Child. *Journal of Information Ethics*, *21*(1), 12–20. http://doi.org/10.3172/JIE.21.1.12

Lin, W.-H., & Lo, H. K. (2015). Highway voting system: Embracing a possible paradigm shift in traffic data acquisition. *Transportation Research Part C: Emerging Technologies*, *56*, 149–160. http://doi.org/10.1016/j.trc.2015.03.025

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *FRONTIERS IN PSYCHOLOGY*, *5*. http://doi.org/10.3389/fpsyg.2014.01298

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. *PSYCHOLOGY & MARKETING*, *32*(6), 601–610. http://doi.org/10.1002/mar.20803

Beteende

Det finns frågor som griper in i flera områden och som inte har någon direkt koppling till ett specifikt fält. En sådan generell fråga rör kopplingen mellan hur den digitala tekniken och möjligheten/hotet att övervaka/övervakas påverkar beteende. Berger et al. (2014) hävdar i artikeln *Surveillance in Digital Space and Changes in User Behaviour* att frågan är dåligt beforskad och skriver att ”the social consequences of a comprehensive surveillance like altering the individual behavior in the digital space have hardly been studied.” I studien som är berördes under rubriken ”Kunskap och beteende bland unga” studeras beteende i termer av nätanvändande och det konkluderas att risken för övervakning medför ett minskat internetanvändande.

En annan artikel (Fuchs 2010) som rör samma område argumenterar för att ökad information och kunskapsbildning för unga angående integritetsfrågor på Internet bidrar till vad som benämns som ”critical information behaviour”. Ett begrepp som definieras som: ”Critical information behaviour involves actions that question the status quo of information systems, it asks if the users really benefit from the standard settings of these systems, and which changes need to be undertaken in order to overcome or lessen power differentials.” (Fuchs 2010, s. 180).

Artikeln *Privacy behaviors after Snowden* (Preibusch 2015) visar att ”privacy beahaviours” visserligen ökade efter Edward Snowdens avslöjande om den långtgående statliga övervakningen som skedde inom ramen för programmet PRISM, men att ökningen var tämligen marginell och inte varade särskilt länge: ”I combined high-resolution data from primary sources that indicate the new public information on PRISM led to momentarily increased interest in privacy and protection. However, the spike was much less than for other news events (such as the royal baby and the U.S. Open golf tournament). It was also less than the increased interest following the removal of privacyenhancing functions in Facebook, Android, and Gmail. While media coverage of PRISM and surveillance was elevated for the 30 weeks following PRISM day, many privacy behaviors faded quickly. Visits to Microsoft’s corporate privacy policy page stayed high, but only certain privacy-related webpages kept larger audiences—those on Snowden and surveillance—while Wikipedia articles about PRISM topics lost their increased readership. Snowden’s revelations brought few new users to privacy-enhancing technologies” (Preibusch 2015, s. 55).

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

4. Artiklar vilka byger på empiriska studier indelade utifrån metod

Vilar mot empiriska studier

Av de sammanlagt 172 artiklarna som ingår i den systematiska litteraturöversikten vilar 56 stycken på empirisk grund, i meningen att det dras slutsatser i artikeln på basis av en systematisk insamling och analys av data. Det ska dock nämnas att det inte varit helt enkelt att göra denna distinktion. Många av artiklarna som inte bedömts ”vila på empirisk grund” redovisar t ex en specifik teknik tämligen ingående (se t ex Lupton 2015) alt. konsekvenser av en specifik lagstiftning för integritet (se t ex Konstadinides 2011) men har inte bedömts presentera ett resultat som bygger på slutsatser av en analys som genomförts av empirin. Vidare bygger många av de artiklar vilka inte har skrivits utifrån egen empiri på tidigare forskning vilken är empirisk. Av de artiklar som vilar på egen empirisk grund har de lite olika angreppssätt för insamling av data. Följande angreppssätt har urskilts och används för att dela upp artiklarna: survey, intervjuer, case studies, mixed methods, dokumentanalys, Internetloggar, experimentella metoder samt övrigt.

Survey 25 st

Amos, C., Zhang, L., & Pentina, I. (2014). Investigating Privacy Perception and Behavior on Weibo. *JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING*, *26*(4), 43–56. http://doi.org/10.4018/joeuc.2014100103

Best, S. J., & Krueger, B. S. (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology & Politics*, *5*(2), 191–212. http://doi.org/10.1080/19331680802294479

Budak, J., Anic, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH*, *26*(1-2, SI), 100–118. http://doi.org/10.1080/13511610.2013.723404

Budak, J., Rajh, E., & Anic, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *JOURNAL OF BALKAN AND NEAR EASTERN STUDIES*, *17*(1), 29–48. http://doi.org/10.1080/19448953.2014.990278

Chaulk, K., & Jones, T. (2011). Online Obsessive Relational Intrusion: Further Concerns About Facebook. *Journal of Family Violence*, *26*(4), 245–254. http://doi.org/10.1007/s10896-011-9360-x

Chen, J. V., Chen, C. C., & Yang, H.-H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *INDUSTRIAL MANAGEMENT & DATA SYSTEMS*, *108*(1-2), 87–106. http://doi.org/10.1108/02635570810844106

Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties. *Analyses of Social Issues and Public Policy*, *5*(1), 263–276. http://doi.org/10.1111/j.1530-2415.2005.00071.x

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *JOURNAL OF GLOBAL INFORMATION MANAGEMENT*, *14*(4), 57–93. http://doi.org/10.4018/jgim.2006100103

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *JOURNAL OF STRATEGIC*

INFORMATION SYSTEMS, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Fox, J., & Warber, K. M. (2014). Social Networking Sites in Romantic Relationships: Attachment, Uncertainty, and Partner Surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3–7. http://doi.org/10.1089/cyber.2012.0667

Helsper, E. J., & Whitty, M. T. (2010). Netiquette within married couples: Agreement about acceptable online behavior and surveillance between partners. *COMPUTERS IN HUMAN BEHAVIOR*, *26*(5), 916–926. http://doi.org/10.1016/j.chb.2010.02.006

Kang, S., & Gearhart, S. (2010). E-Government and Civic Engagement: How is Citizens' Use of City Web Sites Related with Civic Involvement and Political Behaviors? *JOURNAL OF BROADCASTING & ELECTRONIC MEDIA*, *54*(3), 443–462. http://doi.org/10.1080/08838151.2010.498847

Katos, V. (2012). An integrated model for online transactions: illuminating the black box. *Information Management & Computer Security*, *20*(3), 184–206. http://doi.org/10.1108/09685221211247299

Krueger, B. S. (2005). Government surveillance and political participation on the Internet. *SOCIAL SCIENCE COMPUTER REVIEW*, *23*(4), 439–452. http://doi.org/10.1177/0894439305278871

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior and Social Networking*, *15*(10), 521–6. http://doi.org/10.1089/cyber.2012.0125

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *FRONTIERS IN PSYCHOLOGY*, *5*. http://doi.org/10.3389/fpsyg.2014.01298

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. *PSYCHOLOGY & MARKETING*, *32*(6), 601–610. http://doi.org/10.1002/mar.20803

Park, Y. J. (2013a). Digital Literacy and Privacy Behavior Online. *COMMUNICATION RESEARCH*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J. (2013b). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *SOCIAL SCIENCE COMPUTER REVIEW*, *31*(6), 680–702. http://doi.org/10.1177/0894439313485202

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027. http://doi.org/10.1016/j.chb.2012.01.004

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *TELEMATICS AND INFORMATICS*, *29*(2), 233–244. http://doi.org/10.1016/j.tele.2011.08.003

Smith, E., & Lyon, D. (2013). Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance and Society*, *11*(1-2), 190–203. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84881272799&partnerID=tZOtx3y1

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. http://doi.org/10.1108/JICES-01-2014-0004

Tong, S. T. (2013). Facebook use during relationship termination: uncertainty reduction and surveillance. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 788–93. http://doi.org/10.1089/cyber.2012.0549

Xu, H., & Dinev, T. (2012). The security-liberty balance: individuals' attitudes towards internet government surveillance. *Electronic Government, an International Journal*, *9*(1), 46. http://doi.org/10.1504/EG.2012.044778

Intervju 4 st

Draper, N. A. (2012). Group power: Discourses of consumer power and surveillance in group buying websites. *Surveillance and Society*, *9*(4), 394–407. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84873520765&partnerID=tZOtx3y1

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics*, *4*(4), 47–64. http://doi.org/10.1080/19331680801978759

Kim, H., Giacomin, J., & Macredie, R. (2014). A Qualitative Study of Stakeholders' Perspectives on the Social Network Service Environment. *International Journal of Human-Computer Interaction*, *30*(12), 965–976. http://doi.org/10.1080/10447318.2014.925383

Vickery, J. R. (2015). `I don't have anything to hide, but horizontal ellipsis `: the challenges and negotiations of social and mobile media privacy for non-dominant youth. *INFORMATION COMMUNICATION & SOCIETY*, *18*(3, SI), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Case study 4 st

E-safety education: Young people, surveillance and responsibilityBarnard-Wills, D. (2012). E-safety education: Young people, surveillance and responsibility. *CRIMINOLOGY & CRIMINAL JUSTICE*, *12*(3), 239–255. http://doi.org/10.1177/1748895811432957

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Jiang, M., & Okamoto, K. (2014). National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike. *Policy & Internet*, *6*(1), 89–107. http://doi.org/10.1002/1944-2866.POI353

Nuti, S. V, Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The Use of Google Trends in Health Care Research: A Systematic Review. *PLOS ONE*, *9*(10). http://doi.org/10.1371/journal.pone.0109583

Mixed method 3 st

Lukacs, V., & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. *INFORMATION COMMUNICATION & SOCIETY*, *18*(5, SI), 492–508. http://doi.org/10.1080/1369118X.2015.1008540

Park, Y. J., Jang, S. M., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. a. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129–141. http://doi.org/10.1016/j.giq.2015.01.003

Dokumentanalys 2 st

Farinosi, M. (2011). Deconstructing bentham's panopticon: The new metaphors of surveillance in the web 2.0 environment. *TripleC*, *9*(1), 62–76. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZOtx3y1

Haikola, S., & Jonsson, S. (2007). State surveillance on the internet - The Swedish debate and the future role of libraries and LIS. *LIBRI*, *57*(4), 209–218. http://doi.org/10.1515/LIBR.2007.209

Internetloggar 13 st

Arlitt, M., Carlsson, N., Gill, P., Mahanti, A., & Williamson, C. (2011). Characterizing Intelligence Gathering and Control on an Edge Network. *ACM TRANSACTIONS ON INTERNET TECHNOLOGY*, *11*(1). http://doi.org/10.1145/1993083.1993085

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 118–128. http://doi.org/10.1016/j.giq.2015.01.002

Cooper, C. P., Mallon, K. P., Leadbetter, S., Pollack, L. A., & Peipins, L. A. (2005). Cancer Internet search activity on a major search engine, United States 2001-2003. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *7*(3). http://doi.org/10.2196/jmir.7.3.e36

D'Ambrosio, A., Agricola, E., Russo, L., Gesualdo, F., Pandolfi, E., Bortolus, R., … Tozzi, A. E. (2015). Web-Based Surveillance of Public Information Needs for Informing Preconception Interventions. *PLOS ONE*, *10*(4). http://doi.org/10.1371/journal.pone.0122551

Gittelman, S., Lange, V., Crawford, C. A. G., Okoro, C. A., Lieb, E., Dhingra, S. S., & Trimarchi, E. (2015). A New Source of Data for Public Health Surveillance: Facebook Likes. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *17*(4). http://doi.org/10.2196/jmir.3970

Gu, H. y, Chen, B., Zhu, H., Jiang, T., Wang, X., Chen, L., … Jiang, J. (2014). Importance of Internet Surveillance in Public Health Emergency Control and Prevention: Evidence From a Digital Epidemiologic Study During Avian Influenza A H7N9 Outbreaks. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *16*(1). http://doi.org/10.2196/jmir.2911

Gunn, J. F., & Lester, D. (2013). Using google searches on the internet to monitor suicidal behavior. *Journal of Affective Disorders*, *148*(2-3), 411–2. http://doi.org/10.1016/j.jad.2012.11.004

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.)*Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-662-44788-8

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE*, *7*(7). http://doi.org/10.1371/journal.pone.0040200

McEwan, B. (2013). Sharing, caring, and surveilling: an actor-partner interdependence model examination of Facebook relational maintenance strategies. *Cyberpsychology, Behavior and Social Networking*, *16*(12), 863–9. http://doi.org/10.1089/cyber.2012.0717

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

Velardi, P., Stilo, G., Tozzi, A. E., & Gesualdo, F. (2014). Twitter mining for fine-grained syndromic surveillance. *Artificial Intelligence in Medicine*, *61*(3), 153–63. http://doi.org/10.1016/j.artmed.2014.01.002

Experiment 4 st

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *INFORMATION & MANAGEMENT*, *43*(7), 894–903. http://doi.org/10.1016/j.im.2006.08.008

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *JOURNAL OF BUSINESS ETHICS*, *80*(3), 481–498. http://doi.org/10.1007/s10551-007-9432-2

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 633–8. http://doi.org/10.1089/cyber.2013.0585

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. (2009). Effects of electronic mail policies on invasiveness and fairness. *JOURNAL OF MANAGERIAL PSYCHOLOGY*, *24*(6), 502–525. http://doi.org/10.1108/02683940910974107

Övrigt 1 st

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy & Internet*, *6*(4), 360–376. http://doi.org/10.1002/1944-2866.POI375

Samtliga 56 st

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *INFORMATION & MANAGEMENT*, *43*(7), 894–903. http://doi.org/10.1016/j.im.2006.08.008

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *JOURNAL OF BUSINESS ETHICS*, *80*(3), 481–498. http://doi.org/10.1007/s10551-007-9432-2

Amos, C., Zhang, L., & Pentina, I. (2014). Investigating Privacy Perception and Behavior on Weibo. *JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING*, *26*(4), 43–56. http://doi.org/10.4018/joeuc.2014100103

Arlitt, M., Carlsson, N., Gill, P., Mahanti, A., & Williamson, C. (2011). Characterizing Intelligence Gathering and Control on an Edge Network. *ACM TRANSACTIONS ON INTERNET TECHNOLOGY*, *11*(1). http://doi.org/10.1145/1993083.1993085

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Best, S. J., & Krueger, B. S. (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology & Politics*, *5*(2), 191–212. http://doi.org/10.1080/19331680802294479

Budak, J., Anic, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH*, *26*(1-2, SI), 100–118. http://doi.org/10.1080/13511610.2013.723404

Budak, J., Rajh, E., & Anic, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *JOURNAL OF BALKAN AND NEAR EASTERN STUDIES*, *17*(1), 29–48. http://doi.org/10.1080/19448953.2014.990278

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 118–128. http://doi.org/10.1016/j.giq.2015.01.002

Chaulk, K., & Jones, T. (2011). Online Obsessive Relational Intrusion: Further Concerns About Facebook. *Journal of Family Violence*, *26*(4), 245–254. http://doi.org/10.1007/s10896-011-9360-x

Chen, J. V., Chen, C. C., & Yang, H.-H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *INDUSTRIAL MANAGEMENT & DATA SYSTEMS*, *108*(1-2), 87–106. http://doi.org/10.1108/02635570810844106

Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties. *Analyses of Social Issues and Public Policy*, *5*(1), 263–276. http://doi.org/10.1111/j.1530-2415.2005.00071.x

Cooper, C. P., Mallon, K. P., Leadbetter, S., Pollack, L. A., & Peipins, L. A. (2005). Cancer Internet search activity on a major search engine, United States 2001-2003. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *7*(3). http://doi.org/10.2196/jmir.7.3.e36

D'Ambrosio, A., Agricola, E., Russo, L., Gesualdo, F., Pandolfi, E., Bortolus, R., … Tozzi, A. E. (2015). Web-Based Surveillance of Public Information Needs for Informing Preconception Interventions. *PLOS ONE*, *10*(4). http://doi.org/10.1371/journal.pone.0122551

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of

differences between Italy and the United States. *JOURNAL OF GLOBAL INFORMATION MANAGEMENT*, *14*(4), 57–93. http://doi.org/10.4018/jgim.2006100103

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Draper, N. A. (2012). Group power: Discourses of consumer power and surveillance in group buying websites. *Surveillance and Society*, *9*(4), 394–407. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84873520765&partnerID=tZOtx3y1

E-safety education: Young people, surveillance and responsibilityBarnard-Wills, D. (2012). E-safety education: Young people, surveillance and responsibility. *CRIMINOLOGY & CRIMINAL JUSTICE*, *12*(3), 239–255. http://doi.org/10.1177/1748895811432957

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics*, *4*(4), 47–64. http://doi.org/10.1080/19331680801978759

Farinosi, M. (2011). Deconstructing bentham's panopticon: The new metaphors of surveillance in the web 2.0 environment. *TripleC*, *9*(1), 62–76. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZOtx3y1

Fox, J., & Warber, K. M. (2014). Social Networking Sites in Romantic Relationships: Attachment, Uncertainty, and Partner Surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3–7. http://doi.org/10.1089/cyber.2012.0667

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Gittelman, S., Lange, V., Crawford, C. A. G., Okoro, C. A., Lieb, E., Dhingra, S. S., & Trimarchi, E. (2015). A New Source of Data for Public Health Surveillance: Facebook Likes. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *17*(4). http://doi.org/10.2196/jmir.3970

Gu, H. y, Chen, B., Zhu, H., Jiang, T., Wang, X., Chen, L., … Jiang, J. (2014). Importance of Internet Surveillance in Public Health Emergency Control and Prevention: Evidence From a Digital Epidemiologic Study During Avian Influenza A H7N9 Outbreaks. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *16*(1). http://doi.org/10.2196/jmir.2911

Gunn, J. F., & Lester, D. (2013). Using google searches on the internet to monitor suicidal behavior. *Journal of Affective Disorders*, *148*(2-3), 411–2. http://doi.org/10.1016/j.jad.2012.11.004

Haikola, S., & Jonsson, S. (2007). State surveillance on the internet - The Swedish debate and the future role of libraries and LIS. *LIBRI*, *57*(4), 209–218. http://doi.org/10.1515/LIBR.2007.209

Helsper, E. J., & Whitty, M. T. (2010). Netiquette within married couples: Agreement about acceptable online behavior and surveillance between partners. *COMPUTERS IN HUMAN BEHAVIOR*, *26*(5), 916–926. http://doi.org/10.1016/j.chb.2010.02.006

Jiang, M., & Okamoto, K. (2014). National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike. *Policy & Internet*, *6*(1), 89–107. http://doi.org/10.1002/1944-2866.POI353

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.)*Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-662-44788-8

Kang, S., & Gearhart, S. (2010). E-Government and Civic Engagement: How is Citizens' Use of City Web Sites Related with Civic Involvement and Political Behaviors? *JOURNAL OF BROADCASTING & ELECTRONIC MEDIA*, *54*(3), 443–462. http://doi.org/10.1080/08838151.2010.498847

Katos, V. (2012). An integrated model for online transactions: illuminating the black box. *Information Management & Computer Security*, *20*(3), 184–206. http://doi.org/10.1108/09685221211247299

Kim, H., Giacomin, J., & Macredie, R. (2014). A Qualitative Study of Stakeholders' Perspectives on the Social Network Service Environment. *International Journal of Human-Computer Interaction*, *30*(12), 965–976. http://doi.org/10.1080/10447318.2014.925383

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE*, *7*(7). http://doi.org/10.1371/journal.pone.0040200

Krueger, B. S. (2005). Government surveillance and political participation on the Internet. *SOCIAL SCIENCE COMPUTER REVIEW*, *23*(4), 439–452. http://doi.org/10.1177/0894439305278871

Lukacs, V., & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. *INFORMATION COMMUNICATION & SOCIETY*, *18*(5, SI), 492–508. http://doi.org/10.1080/1369118X.2015.1008540

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior and Social Networking*, *15*(10), 521–6. http://doi.org/10.1089/cyber.2012.0125

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *FRONTIERS IN PSYCHOLOGY*, *5*. http://doi.org/10.3389/fpsyg.2014.01298

McEwan, B. (2013). Sharing, caring, and surveilling: an actor-partner interdependence model examination of Facebook relational maintenance strategies. *Cyberpsychology, Behavior and Social Networking*, *16*(12), 863–9. http://doi.org/10.1089/cyber.2012.0717

Nuti, S. V, Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The Use of Google Trends in Health Care Research: A Systematic Review. *PLOS ONE*, *9*(10). http://doi.org/10.1371/journal.pone.0109583

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 633–8. http://doi.org/10.1089/cyber.2013.0585

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. *PSYCHOLOGY & MARKETING*, *32*(6), 601–610. http://doi.org/10.1002/mar.20803

Park, Y. J. (2013a). Digital Literacy and Privacy Behavior Online. *COMMUNICATION RESEARCH*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J. (2013b). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *SOCIAL SCIENCE COMPUTER REVIEW*, *31*(6), 680–702. http://doi.org/10.1177/0894439313485202

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy & Internet*, *6*(4), 360–376. http://doi.org/10.1002/1944-2866.POI375

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027. http://doi.org/10.1016/j.chb.2012.01.004

Park, Y. J., Jang, S. M., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. (2009). Effects of electronic mail policies on invasiveness and fairness. *JOURNAL OF MANAGERIAL PSYCHOLOGY*, *24*(6), 502–525. http://doi.org/10.1108/02683940910974107

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. a. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129–141. http://doi.org/10.1016/j.giq.2015.01.003

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *TELEMATICS AND INFORMATICS*, *29*(2), 233–244. http://doi.org/10.1016/j.tele.2011.08.003

Smith, E., & Lyon, D. (2013). Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance and Society*, *11*(1-2), 190–203. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84881272799&partnerID=tZOtx3y1

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. http://doi.org/10.1108/JICES-01-2014-0004

Tong, S. T. (2013). Facebook use during relationship termination: uncertainty reduction and surveillance. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 788–93. http://doi.org/10.1089/cyber.2012.0549

Velardi, P., Stilo, G., Tozzi, A. E., & Gesualdo, F. (2014). Twitter mining for fine-grained syndromic surveillance. *Artificial Intelligence in Medicine*, *61*(3), 153–63. http://doi.org/10.1016/j.artmed.2014.01.002

Vickery, J. R. (2015). `I don't have anything to hide, but horizontal ellipsis `: the challenges and negotiations of social and mobile media privacy for non-dominant youth. *INFORMATION COMMUNICATION & SOCIETY*, *18*(3, SI), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Xu, H., & Dinev, T. (2012). The security-liberty balance: individuals' attitudes towards internet government surveillance. *Electronic Government, an International Journal*, *9*(1), 46. http://doi.org/10.1504/EG.2012.044778

Statens offentliga utredningar 2016

Kronologisk förteckning

1. Statens bredbandsinfrastruktur som resurs. N.
2. Effektiv vård. S.
3. Höghastighetsjärnvägens finansiering och kommersiella förutsättningar. N.
4. Politisk information i skolan – ett led i demokratiuppdraget. U.
5. Låt fler forma framtiden! Del A + B. Ku.
6. Framtid sökes – Slutredovisning från den nationella samordnaren för utsatta EU-medborgare. S.
7. Integritet och straffskydd. Ju.
8. Ytterligare åtgärder mot penningtvätt och finansiering av terrorism. Fjärde penningstvättsdirektivet – samordning – ny penningtvättslag – m.m. Del 1 + 2. Fi.
9. Plats för nyanlända i fler skolor. U.
10. EU på hemmaplan. Ku.
11. Olika vägar till föräldraskap. Ju.
12. Ökade möjligheter till modersmålsundervisning och studiehandledning på modersmål. U.
13. Palett för ett stärkt civilsamhälle. Ku.
14. En översyn av tobakslagen. Nya steg mot ett minskat tobaksbruk. S.
15. Arbetsklausuler och sociala hänsyn i offentlig upphandling – ILO:s konvention nr 94 samt en internationell jämförelse. Fi.
16. Kunskapsläget på kärnavfallsområdet 2016. Risker, osäkerheter och framtidsutmaningar. M.
17. EU:s reviderade insolvensförordning m.m. Ju.
18. En ny strafftidslag. Ju.
19. Barnkonventionen blir svensk lag. S.
20. Föräldraledighet för statsråd? Fi.
21. Ett klimatpolitiskt ramverk för Sverige. M.
22. Möjlighet att begränsa eller förbjuda odling av genetiskt modifierade växter i Sverige. M.
23. Beskattning av incitamentsprogram. Fi.
24. En ändamålsenlig kommunal redovisning. Fi.
25. Likvärdigt, rättssäkert och effektivt – ett nytt nationellt system för kunskapsbedömning. Del 1 + 2. U.
26. På väg mot en ny politik för Sveriges landsbygder – landsbygdernas utveckling, möjligheter och utmaningar. N.
27. Som ett brev på posten. Postbefordran och pristak i ett digitaliserat samhälle. N.
28. Vägen till självkörande fordon – försöksverksamhet. N.
29. Trygghet och attraktivitet – en forskarkarriär för framtiden. U.
30. Människorna, medierna & marknaden. Medieutredningens forskningsantologi om en demokrati i förändring. Ku.
31. Fastighetstaxering av anläggningar för el- och värmeproduktion. Fi.
32. En trygg dricksvattenförsörjning. Del 1 + 2 och Sammanfattning. N.
33. Ett bonus–malus-system för nya lätta fordon. Fi.
34. Revisorns skadeståndsansvar. Ju.
35. Vägen in till det svenska skolväsendet. U.
36. Medverkan av tjänsteleverantörer i ärenden om uppehålls- och arbetstillstånd. UD.
37. Rätten till en personförsäkring. – ett stärkt konsumentskydd. Ju.
38. Samling för skolan. Nationella målsättningar och utvecklingsområden för kunskap och likvärdighet. U.

39. Polis i framtiden
– polisutbildningen som högskole-utbildning. Ju.
40. Straffrättsliga åtgärder mot deltagande i en väpnad konflikt till stöd för en terroristorganisation. Ju.
41. Hur står det till med den personliga integriteten?
– en kartläggning av Integritets-kommittén. Ju.

Statens offentliga utredningar 2016

Systematisk förteckning

Finansdepartementet

Ytterligare åtgärder mot penningtvätt och finansiering av terrorism. Fjärde penningtvättsdirektivet – samordning – ny penningtvättslag – m.m. Del 1 + 2. [8]

Arbetsklausuler och sociala hänsyn i offentlig upphandling – ILO:s konvention nr 94 samt en internationell jämförelse. [15]

Föräldraledighet för statsråd? [20]

Beskattning av incitamentsprogram. [23]

En ändamålsenlig kommunal redovisning. [24]

Fastighetstaxering av anläggningar för el- och värmeproduktion. [31]

Ett bonus–malus-system för nya lätta fordon. [33]

Justitiedepartementet

Integritet och straffskydd. [7]

Olika vägar till föräldraskap. [11]

EU:s reviderade insolvensförordning m.m. [17]

En ny strafftidslag. [18]

Revisorns skadeståndsansvar. [34]

Rätten till en personförsäkring – ett stärkt konsumentskydd. [37]

Polis i framtiden – polisutbildningen som högskoleutbildning. [39]

Straffrättsliga åtgärder mot deltagande i en väpnad konflikt till stöd för en terroristorganisation. [40]

Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén. [41]

Kulturdepartementet

Låt fler forma framtiden! Del A + B. [5]

EU på hemmaplan. [10]

Palett för ett stärkt civilsamhälle. [13]

Människorna, medierna & marknaden Medieutredningens forskningsantologi om en demokrati i förändring. [30]

Miljö- och energidepartementet

Kunskapsläget på kärnavfallsområdet 2016. Risker, osäkerheter och framtidsutmaningar. [16]

Ett klimatpolitiskt ramverk för Sverige. [21]

Möjlighet att begränsa eller förbjuda odling av genetiskt modifierade växter i Sverige. [22]

Näringsdepartementet

Statens bredbandsinfrastruktur som resurs. [1]

Höghastighetsjärnvägens finansiering och kommersiella förutsättningar. [3]

På väg mot en ny politik för Sveriges landsbygder – landsbygdernas utveckling, möjligheter och utmaningar. [26]

Som ett brev på posten. Postbefordran och pristak i ett digitaliserat samhälle. [27]

Vägen till självkörande fordon – försöksverksamhet. [28]

En trygg dricksvattenförsörjning. Del 1 + 2 och Sammanfattning. [32]

Socialdepartementet

Effektiv vård. [2]

Framtid sökes – Slutredovisning från den nationella samordnaren för utsatta EU-medborgare. [6]

En översyn av tobakslagen. Nya steg mot ett minskat tobaksbruk. [14]

Barnkonventionen blir svensk lag. [19]

Utbildningsdepartementet

Politisk information i skolan – ett led i demokratiuppdraget. [4]

Plats för nyanlända i fler skolor. [9]

Ökade möjligheter till modersmåls-undervisning och studiehandledning på modersmål. [12]

Likvärdigt, rättssäkert och effektivt – ett nytt nationellt system för kunskaps-bedömning. Del 1 + 2. [25]

Trygghet och attraktivitet – en forskarkarriär för framtiden. [29]

Vägen in till det svenska skolväsendet. [35]

Samling för skolan. Nationella målsätt-ningar och utvecklingsområden för kunskap och likvärdighet. [38]

Utrikesdepartementet

Medverkan av tjänsteleverantörer i ärenden om uppehålls- och arbetstillstånd. [36]