Säkrare verifiering av identitet

Volym 1

Betänkande av Utredningen om säkrare verifiering av identitet

Stockholm 2026

STATENS OFFENTLIGA UTREDNINGAR

SOU 2026:55

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Multiply Solutions
Tryck och remisshantering: Multiply Solutions, Stockholm 2026

ISBN 978-91-525-1597-6 (tryck)
ISBN 978-91-525-1598-3 (pdf)
ISSN 0375-250X

Till statsrådet Elisabeth Svantesson

Regeringen beslutade den 6 mars 2025 att ge en särskild utredare i uppdrag att lämna förslag som stärker kopplingen mellan fastställd grundidentitet och verifiering av identitet (dir. 2025:22). Syftet med uppdraget är att skapa en effektivare och säkrare process vid verifiering av identitet som utgår från biometriska uppgifter. Förslagen ska bidra till en effektiv, tillförlitlig och ändamålsenlig identitetsförvaltning i Sverige.

Kammarrättslagmannen Peder Liljeqvist förordnades till särskild utredare den 6 mars 2025. Som huvudsekreterare anställdes rådmannen Alexander Warnolf från den 10 mars 2025 och som sekreterare anställdes (numera) rådmannen Jenny Björstrand från den 1 april 2025.

Som experter att biträda utredningen förordnades den 2 maj 2025 numera rättssakkunniga Åsa Brundin, Justitiedepartementet, experten Peter Cederholm, Migrationsverket, verksamhetsutvecklaren Azize Cuydur, Försäkringskassan, juristen Anna Döös, Myndigheten för digital förvaltning, dåvarande rättssakkunniga numera kanslirådet Alicia Eklund, Finansdepartementet, ämnesrådet Cecilia Eriksson, Finansdepartementet, seniora verksjuristen Fredrik Hugo, Säkerhetspolisen, it- och informationssäkerhetsspecialisten Mats Juhlén, Integritetsskyddsmyndigheten, verksamhetsutvecklaren Kristin Markroth Bergh, Polismyndigheten, numera kanslirådet Charlotte Roth Olanders, Justitiedepartementet, rättsliga experten Gunnar Svensson, Skatteverket och utvecklingsstrategen Tobias Wijk, Skatteverket. Gunnar Svensson entledigades den 1 september 2025 och samma dag förordnades rättsliga experten Therese Olofsson Friberg, Skatteverket att vara expert i utredningen. Den 13 januari 2026 entledigades Alicia Eklund. Samma dag förordnades rättssakkunniga Amanda Hägglund, Finansdepartementet att vara expert i utredningen.

Utredningen redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar.

Utredningen om säkrare verifiering av identitet överlämnar härmed betänkandet *Säkrare verifiering av identitet* (SOU 2026:55). Vårt arbete är i och med detta slutfört.

Stockholm i augusti 2026

Peder Liljeqvist

Alexander Warnolf
Jenny Björstrand

Innehåll

VOLYM 1

Sammanfattning 25

Summary 37

1 Författningsförslag 47

1.1 Förslag till lag om biometrisk verifiering av identitet 47

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400) 51

2 Utredningens uppdrag och arbete samt betänkandets disposition 53

2.1 Våra direktiv 53

2.2 Utgångspunkter och avgränsningar 54

2.3 Vårt arbete 55

2.4 Betänkandets disposition 55

Del 1 – Allmänna utgångspunkter

3 Identitet 61

3.1 Inledning 61

3.2 Identitetsbegreppet 61

3.3 Grundidentitet 63

4 Biometri samt biometriska underlag, uppgifter och mallar 65

4.1 Inledning 65

4.2 Biometri 65

4.3 Biometriska underlag 66

4.4 Biometriska uppgifter 67

4.5 Biometriska mallar 69

5 Allmänt om dataskydd och grundläggande rättigheter 73

5.1 Inledning 73

5.2 Dataskydd 74
5.2.1 Dataskyddsförordningen 74
5.2.2 Dataskyddslagen 75
5.2.3 Grundläggande principer för personuppgiftsbehandling 76
5.2.4 Särskilt om känsliga personuppgifter 79
5.2.5 Särskilt om person- och samordningsnummer 80
5.2.6 Dataskyddsdirektivet och brottsdatalagen 81

5.3 Skydd för den personliga integriteten 82
5.3.1 Regeringsformen 82
5.3.2 Europakonventionen 84
5.3.3 EU:s rättighetsstadga 85

6 Ärenden där en identitet kan behöva etableras 87

6.1 Inledning 87

6.2 Migrationsverket och utlandsmyndigheterna 88
6.2.1 Uppehållstillstånd 88
6.2.2 Schengenviseringar och nationella viseringar 89
6.2.3 Förslag om registrering av EES-medborgare i vissa fall 91

6.3 Polismyndigheten 92
6.3.1 Gränskontroller 92
6.3.2 Inre utlänningskontroller 93

6.4 Skatteverket ... 94
6.4.1 Folkbokföring ... 95
6.4.2 Tilldelning av samordningsnummer ... 96

7 Verifiering av identitet och identifiering ... 99

7.1 Inledning ... 99

7.2 Verifiering av identitet ... 101
7.2.1 Närmare om begreppet verifiering ... 102
7.2.2 Verifiering i förhållande till beviskrav ... 105

7.3 Identifiering ... 107
7.3.1 Närmare om begreppet identifiering ... 107
7.3.2 Möjlighet att identifiera en person i olika sammanhang ... 109

7.4 Metoder för att verifiera identitet ... 112
7.4.1 Identifiering som metod för att verifiera identitet ... 112
7.4.2 Verifiering av identitet mot handlingar ... 114
7.4.3 Verifiering mot uppgifter i ett register ... 126

8 Registrering av uppgifter i vissa register ... 135

8.1 Inledning ... 135

8.2 Allmänt om registrering av uppgifter ... 136
8.2.1 Behovet varierar utifrån ärendeslaget ... 137
8.2.2 Uppgifter från EU-gemensamma informationssystem ... 139

8.3 Registrering av alfanumeriska uppgifter ... 142
8.3.1 Ärenden på utlänningsrättens område ... 143
8.3.2 Ärenden i folkbokföringsverksamheten ... 144
8.3.3 Utfärdande av pass och nationellt identitetskort ... 146

8.4 Registrering av biometriska uppgifter ... 147
8.4.1 Ärenden på utlänningsrättens område ... 148
8.4.2 Ärenden i folkbokföringsverksamheten ... 153
8.4.3 Utfärdande av pass och nationellt identitetskort ... 154

9 Identitetsmissbruk – orsaker och konsekvenser 157

9.1 Inledning 157

9.2 Problembild 157
9.2.1 Översikt av olika typer av identitetsmissbruk 158
9.2.2 Felaktiga och falska identiteter 159
9.2.3 Multipla identiteter 167
9.2.4 Utnyttjande av identiteter 170
9.2.5 Omfattningen av identitetsmissbruk 172

10 Tänkbara åtgärder för säkrare verifiering av identitet 177

10.1 Inledning 177

10.2 Åtgärder av generell karaktär 178
10.2.1 Kompetenshöjande åtgärder och metodutveckling 178
10.2.2 Högre beviskrav i fråga om identitet 179
10.2.3 Utökade möjligheter att kräva personlig inställelse 180

10.3 Åtgärder när en identitet behöver etableras 182
10.3.1 Utökad användning av biometriska uppgifter 183
10.3.2 Utökat stöd för att lagra biometriska uppgifter 188

10.4 Utökad användning av biometri är nödvändig 190

10.5 Verifiering mot handlingar 192
10.5.1 Tillgång till identitetshandlingar 193
10.5.2 Utökad användning av biometriska uppgifter 195

10.6 Verifiering mot befintliga register 199
10.6.1 Stöd för fler aktörer att använda lagrade biometriska uppgifter 200
10.6.2 Utökat informationsutbyte mellan Polismyndigheten, Migrationsverket och Skatteverket 206
10.6.3 Utökad användning av EU-gemensamma system 208

10.7 Verifiering mot ett nytt identitetsindex 213
10.7.1 Grunderna i ett system med ett identitetsindex och omständigheter att beakta 214
10.7.2 Begreppet identitetsindex 217
10.7.3 En sammanhållen syn på information om identiteter 218
10.7.4 Ett identitetsindex kan främja ”en person, en identitet” 220
10.7.5 Många aktörer bör kunna använda systemet 221
10.7.6 Ett identitetsindex bör byggas upp från grunden 223

10.8 Sammanfattande bedömning 225

Del 2 – Två huvudalternativ

11 Uppgifter som ett identitetsindex bör innehålla 229

11.1 Inledning 229

11.2 Utgångspunkter 229

11.3 Ett index bör innehålla en unik identitetsnyckel 231
11.3.1 En nyckel som baseras på person- eller samordningsnummer 231
11.3.2 En nyckel som baseras på biometriska underlag 232
11.3.3 En identitetsnyckel baserad på ett UUID 234

11.4 Uppgifter som bör kopplas till en identitetsnyckel 236
11.4.1 Identitetsuppgifter 236
11.4.2 Kön 237
11.4.3 Person- och samordningsnummer 239
11.4.4 Migrationsverkets individnummer 240
11.4.5 Biometriska underlag och biometriska uppgifter 242
11.4.6 Särskilt om sekretessmarkering 250

12 Personkategorier som bör omfattas 253

12.1 Inledning 253

12.2 Utgångspunkter 253
12.2.1 Hemvist i Sverige 254
12.2.2 Att vara bosatt i Sverige 255
12.2.3 Annan anknytning till Sverige 257

12.3 Personkategorier som det finns ett behov av att registrera i ett identitetsindex 259
12.3.1 Personer som är eller har varit folkbokförda i Sverige 259
12.3.2 Personer som har tilldelats ett samordningsnummer 261
12.3.3 Personer med uppehållstillstånd 263
12.3.4 Personer med ställning som varaktigt bosatta 266
12.3.5 Svenska medborgare 267
12.3.6 Personer med kvalificerade skyddsidentiteter 269

12.4 Personkategorier som det saknas ett behov av att registrera i ett identitetsindex 271
12.4.1 Barn som inte har fyllt sex år 271
12.4.2 Personer som ansöker om internationellt skydd 273
12.4.3 Personer som vistas olagligen i Sverige 277
12.4.4 Personer som har beviljats visering 280
12.4.5 Personer med uppehållsrätt som saknar en identitetsbeteckning 281
12.4.6 Diplomatisk personal 283

13 Registrering av en identitetsnyckel 287

13.1 Inledning 287

13.2 Utgångspunkter 287
13.2.1 Kontroll av om en individ är registrerad i ett identitetsindex 287
13.2.2 Kontroll av eventuell sekretessmarkering 289
13.2.3 Inget beviskrav avseende identitet 290

13.2.4 Registrering i samband med att biometriska underlag tas upp vid handläggningen av ett ärende ... 291
13.2.5 Registrering på frivillig basis ... 294
13.2.6 En möjlighet för andra myndigheter än Skatteverket, Migrationsverket och Polismyndigheten att initiera en registrering i ett identitetsindex ... 297
13.2.7 Rättsligt stöd för att ta upp och behandla biometriska underlag och uppgifter ... 299
13.2.8 Personkategorier som bör undantas ... 301

13.3 Ärenden i vilka en identitetsnyckel bör skapas ... 302
13.3.1 Medborgarskapsärenden ... 302
13.3.2 Utfärdande av pass ... 306
13.3.3 Utfärdande av ett statligt identitetskort ... 309
13.3.4 Utfärdande av en statlig e-legitimation ... 313
13.3.5 Utfärdande av uppehållstillståndskort ... 314
13.3.6 Folkbokföringsärenden ... 316
13.3.7 Ärenden om samordningsnummer ... 323
13.3.8 Ärenden om kvalificerad skyddsidentitet ... 330
13.3.9 Andra ärendeslag som kan övervägas ... 333

13.4 Ansvar för att skapa en identitetsnyckel ... 338
13.4.1 Ansvaret bör fördelas utifrån ärendeslag ... 338
13.4.2 Särskilt om utlandsmyndigheterna ... 343

14 Uppdatering av uppgifter i ett identitetsindex ... 347

14.1 Inledning ... 347

14.2 Utgångspunkter ... 347
14.2.1 Vad vi avser med att en uppgift uppdateras ... 347
14.2.2 Vikten av objektivt korrekta uppgifter ... 350

14.3 Uppdatering för att uppgifter ska vara aktuella ... 351
14.3.1 Översiktlig bedömning av när uppgifter bör uppdateras ... 352
14.3.2 Identitetsuppgifter ... 354
14.3.3 Särskilt om sekretessmarkering ... 357
14.3.4 Person- och samordningsnummer ... 357

14.3.5 Migrationsverkets individnummer ... 359
14.3.6 Ansiktsbild och biometriska uppgifter ... 360
14.3.7 Kontroller när en uppgift ska uppdateras ... 366

14.4 Rättelse och radering av felaktiga uppgifter ... 369
14.4.1 Rättelse och radering enligt dataskyddsförordningen ... 371
14.4.2 Ansvar för att rätta eller radera en felaktig uppgift ... 376
14.4.3 Kontroller när en uppgift behöver rättas eller raderas ... 383
14.4.4 Underrättelseskyldighet avseende felaktiga uppgifter ... 384

15 Radering av en individ i ett identitetsindex ... 389

15.1 Inledning ... 389

15.2 Radering på grund av ändrade förhållanden ... 390
15.2.1 När den registrerade avlider ... 390
15.2.2 När omständigheterna som föranledde registreringen ändras ... 392
15.2.3 När en kvalificerad skyddsidentitet upphör att gälla ... 396

15.3 Rätten till radering ... 397

15.4 Radering på initiativ av tillsynsmyndigheten ... 398

15.5 Särskilda skäl för att radera en individ ... 399

16 Ett identitetsindex förenlighet med dataskydd m.m. ... 403

16.1 Inledning ... 403

16.2 Utgångspunkter ... 404
16.2.1 Verksamhet med ett identitetsindex ... 404

16.3 Rättslig grund för att behandla personuppgifter i verksamheten med ett identitetsindex ... 406
16.3.1 Uppgift av allmänt intresse och myndighetsutövning ... 406

16.4 Behandling av känsliga personuppgifter i verksamheten med ett identitetsindex 410
16.4.1 Behandling av biometriska uppgifter 410
16.4.2 Undantag krävs för behandling av biometriska uppgifter 411
16.4.3 Viktigt allmänt intresse 412

16.5 Förhållande till grundläggande rättigheter 417
16.5.1 Behandling av biometriska uppgifter i verksamhet med ett identitetsindex inskränker vissa rättigheter 417
16.5.3 Inskränkningarna har ett legitimt syfte 422
16.5.4 Verksamheten med ett identitetsindex bör regleras i lag 425

16.6 Sammanfattande slutsatser 427

17 Proportionalitetsbedömning avseende ett identitetsindex 429

17.1 Inledning 429

17.2 Utgångspunkter för bedömningen 430

17.4 Faktorer till men för den personliga integriteten 431
17.4.1 Ett stort antal personer skulle komma att omfattas 431
17.4.2 Uppgifter om barn kommer att behandlas 432
17.4.3 Utökad upptagning av biometriska underlag 433
17.4.4 Utökad lagring av biometriska uppgifter 434
17.4.5 Utökad behandling av biometriska uppgifter 436
17.4.6 Begränsade möjligheter att undvika en registrering 436

17.5 Faktorer som minskar integritetsintrånget 438
17.5.1 En avgränsad personkrets, utifrån syftet med ett index, och ett tydligt behov 438
17.5.2 En begränsad uppsättning uppgifter 444
17.5.3 Personuppgifternas karaktär 446
17.5.4 Behandlingen av personuppgifter vid registrering, uppdatering, rättelse och radering är förutsebar 449

17.5.5 Behandling skulle ske för huvudsakligen samma syften som i det ärendeslag som föranleder en registrering 451

17.6 Sammantagen bedömning 451
17.6.1 Verksamhet med ett identitetsindex medför vissa inskränkningar i grundläggande rättigheter… 452
17.6.2 … men motiveras av ett starkt allmänt intresse .. 454

18 Allmänt om användning av ett identitetsindex 459

18.1 Inledning 459

18.2 Identifiering 460
18.2.1 När identifiering bör få användas 460
18.2.2 Uppgifter som behöver göras tillgängliga 468

18.3 Verifiering med hjälp av biometriska uppgifter 471
18.3.1 Steg 1 – Rätt individ behöver lokaliseras 472
18.3.2 Steg 2 – Upptagning av ansiktsbild 473
18.3.3 Steg 3 – Jämförelse av biometriska uppgifter 475
18.3.4 Steg 4 – Verifiering av identitet 477

18.4 Verifiering med hjälp av en ansiktsbild 479
18.4.1 Steg 1 – Rätt individ behöver lokaliseras 480
18.4.2 Steg 2 – Verifiering av identitet 481

18.5 Efterföljande behandling av ansiktsbilder och biometriska uppgifter 483

18.6 Åtkomst och utlämnande av uppgifter 484
18.6.1 Elektroniskt utlämnande bör vara tillåtet 485
18.6.2 Allmänt om direktåtkomst respektive annat elektroniskt utlämnande 485
18.6.3 Formerna för utlämnande bör regleras särskilt ... 488

19 Handlingar som är lämpliga för biometrisk verifiering av identitet 493

19.1 Inledning 493

19.2 Utgångspunkter 494

19.2.1 Handlingen behöver innehålla ett lagringsmedium ... 497

19.3 Handlingar som kan vara aktuella att använda ... 500
19.3.1 Hemlandspass ... 500
19.3.2 Identitetskort ... 503
19.3.3 Uppehållstillståndskort ... 508
19.3.4 Främlingspass och resedokument ... 513
19.3.5 Uppehållskort samt bevis om uppehållsstatus och bevis för gränsarbetare ... 516
19.3.6 Elektroniska identitetshandlingar ... 517

19.4 Sammanfattande slutsatser ... 521

20 Allmänt om biometrisk verifiering av identitet mot handlingar ... 525

20.1 Inledning ... 525

20.2 Biometriska uppgifter som bör få användas ... 525
20.2.1 Generella avgränsningar ... 526
20.2.2 Rättsliga begränsningar ... 527
20.2.3 Tekniska faktorer ... 528
20.2.4 Underlag i form av en synlig ansiktsbild ... 530
20.2.5 Integritetsaspekter ... 531

20.3 Upptagning av biometriska underlag ... 532

20.4 Begränsning till barn över sex år ... 533

20.5 Uppgifter som en myndighet bör få tillgång till vid biometrisk verifiering mot handlingar ... 534

20.6 Efterföljande behandling av biometriska underlag och biometriska uppgifter ... 537

21 Användning av biometrisk verifiering ... 539

21.1 Inledning ... 539

21.2 Användningen behöver regleras i lag ... 540

21.3 Aktörer som bör omfattas ... 542
21.3.1 Myndigheter ... 543

21.3.2 Privata aktörer ... 550

21.4 Brottsbekämpande verksamhet ... 562

21.5 Verifiering med hjälp av biometriska uppgifter ... 568
21.5.1 Handläggning av ett ärende enligt förvaltningslagen ... 569
21.5.2 Identitetskontroller i annat fall ... 579
21.5.3 En rätt att vidta tvångsåtgärder bör inte övervägas ... 583

21.6 Verifiering med hjälp av en ansiktsbild mot ett identitetsindex ... 584

21.7 Förenlighet med dataskydd och grundläggande rättigheter ... 586
21.7.1 Rättslig grund för att behandla personuppgifter ... 587
21.7.2 Undantag för behandling av biometriska uppgifter ... 589
21.7.3 Proportionalitetsbedömning ... 592

22 Jämförelse av de två huvudalternativen ... 601

22.1 Inledning ... 601

22.2 Personkretsar som kan fångas upp ... 602
22.2.1 Svenska medborgare ... 602
22.2.2 EES-medborgare ... 603
22.2.3 Tredjelandsmedborgare ... 604

22.3 Krav på medverkan ... 606

22.4 Identifiering av okända personer ... 607

22.5 Biometriska underlag som kan användas ... 607

22.6 Möjlighet att motverka olika former av identitetsmissbruk ... 608

22.7 Särskilt om kvalificerade skyddsidentiteter och personer med sekretessmarkering i folkbokföringen ... 609

22.8 Olika aktörers möjlighet att verifiera identitet ... 610

22.9 Koppling till en grundidentitet 611
22.10 Rättslig och teknisk komplexitet 613
22.11 Integritetspåverkan 617
22.12 Implementeringstid 620
22.13 Kostnader 621
22.14 Sammantagen bedömning 622
22.14.1 Ett system med ett identitetsindex 623
22.14.2 Biometrisk verifiering av identitet mot handlingar 625
22.14.3 Sammanfattande slutsats 627

VOLYM 2

Del 3 – Ett system för biometrisk verifiering av identitet

23 En ny lag om biometrisk verifiering av identitet 631
23.1 Inledning 631
23.2 En särskild lag ska införas 631
23.2.1 En lag om biometrisk verifiering av identitet ska införas 632
23.2.2 Lagens syfte 634
23.3 Den nya lagen ska komplettera befintliga möjligheter till biometrisk verifiering av identitet mot handlingar 636
23.4 Undantag för brottsbekämpande verksamhet 638
23.5 Definitioner av vissa begrepp 641
23.5.1 Barn 641
23.5.2 Identitet 642
23.5.3 Biometriska underlag 644
23.5.4 Biometriska uppgifter 645
23.5.5 Biometrisk verifiering av identitet 647
23.5.6 Myndighet 648
23.6 En generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar 649

23.6.1 En möjlighet, inte en skyldighet 649
23.6.2 Typer av handlingar som ska få användas 653
23.6.3 Grundläggande förutsättningar 655
23.6.4 En skyldighet att lämna biometriska underlag för kontroll mot dem som är lagrade i en handling 658

23.7 Konsekvenser av att verifieringen inte visat att den påstådda identiteten är riktig 664

23.8 Åtgärder för att förmå den enskilde att medverka till biometrisk verifiering enligt den nya lagen 667
23.8.1 Begränsning till handläggningen av ett ärende 668
23.8.2 En särskild bestämmelse om föreläggande ska införas 670
23.8.3 Förutsättningar för att meddela ett föreläggande 673
23.8.4 Vem ett föreläggande ska kunna rikta sig till 675
23.8.5 Åtgärder som den enskilde kan föreläggas att vidta 677
23.8.6 Konsekvenser av att ett föreläggande inte följs ... 680

23.9 Rätt att meddela föreskrifter 684

24 Dataskydd 687

24.1 Inledning 687

24.2 Bestämmelser om behandling av personuppgifter ska införas i den nya lagen 687

24.3 De nya bestämmelserna ska komplettera den allmänna dataskyddslagstiftningen 689

24.4 Tillämpningsområde för bestämmelser om personuppgiftsbehandling 691

24.5 Förhållandet till befintliga registerförfattningar 694

24.6 Personuppgiftsansvar 697

24.7 Personuppgiftsbiträde 701

24.8 Ändamål för personuppgiftsbehandling 703

24.9 Efterföljande behandling av biometriska underlag och biometriska uppgifter 706

24.10 Tillgång till personuppgifter 707

24.11 Enskildas rättigheter 709
24.11.1 Information och tillgång till personuppgifter 709
24.11.2 Rättelse och radering 711
24.11.3 Rätten att göra invändningar 711

24.12 Åtkomst och utlämnande av uppgifter 714

25 Sekretess 719

25.1 Inledning 719

25.2 Sekretess vid användning av den verifierande myndighetens system 720
25.2.1 Alfanumeriska uppgifter 721
25.2.2 Biometriska underlag och biometriska uppgifter 724

25.3 Sekretess vid användning av myndighetsgemensamma system 729
25.3.1 Särskilt om teknisk bearbetning 731
25.3.2 Utlämnande av uppgifter till en tekniskt ansvarig aktör 734
25.3.3 Skydd för uppgifter hos en tekniskt ansvarig aktör 737
25.3.4 Utlämnande av uppgifter från en tekniskt ansvarig aktör till den verifierande myndigheten 738

25.4 Sammanfattande slutsatser 740

26 Processuella frågor 743

26.1 Inledning 743

26.2 Rätten att överklaga enligt förvaltningslagen 743
26.2.1 Beslut 744
26.2.2 Antas påverka någons situation 744
26.2.3 På ett inte obetydligt sätt 745

26.3 Förvaltningsbeslut ... 745
26.3.1 Biometrisk verifiering vid handläggningen av ett ärende ... 746
26.3.2 Biometrisk verifiering vid genomförande av identitetskontroller ... 751

26.4 Beslut enligt regelverket om dataskydd ... 753
26.4.1 Personuppgiftsansvariga myndigheters beslut ... 753
26.4.2 Tillsynsmyndighetens beslut ... 754
26.4.3 Vissa andra beslut ... 754
26.4.4 Behov saknas av särskilda överklagandebestämmelser ... 755

27 Tekniska frågor ... 757

27.1 Inledning ... 757

27.2 Tekniska standarder för uppgifter i handlingar ... 760

27.3 En verifieringsprocess som bygger på egna tekniska system ... 762
27.3.1 Översikt av de olika stegen i verifieringsprocessen ... 764
27.3.2 Nödvändiga systemkomponenter och särskilda risker ... 764

27.4 En verifieringsprocess som bygger på ett system med myndighetsgemensamma komponenter ... 765
27.4.1 Närmare om verifieringsprocessen ... 767
27.4.2 Nödvändiga systemkomponenter ... 776
27.4.3 Särskilt om koppling till en svensk identitetsbeteckning och till Migrationsverkets individnummer ... 779

27.5 Internationell utblick – GOV.UK One Login ... 782

27.6 Sammanfattande slutsatser ... 783

28 Informations- och cybersäkerhet samt säkerhetsskydd . 791

28.1 Inledning ... 791

28.2 Informations- och cybersäkerhet ... 792
28.2.1 Cybersäkerhetslagen (NIS2-direktivet) ... 793
28.2.2 CER-direktivet ... 797
28.2.3 Dataskyddsförordningen ... 799
28.2.4 Vissa särskilda risker och åtgärder för att motverka dem ... 799
28.2.5 Sammanfattning ... 807

28.3 Säkerhetsskydd ... 808
28.3.1 Allmänt om säkerhetsskydd ... 809
28.3.2 Tillhandahållande av ett myndighetsgemensamt system ... 810
28.3.3 Uppgifter som förekommer vid biometrisk verifiering ... 812
28.3.4 Sammanfattning ... 814

29 Ansvarsfördelning ... 817

29.1 Inledning ... 817

29.2 Ansvar för biometrisk verifiering av identitet ... 817

29.3 Genomförande av våra förslag förutsätter inte en myndighetsgemensam teknisk lösning ... 819

29.4 En eller flera privata aktörer bör inte ansvara för en myndighetsgemensam teknisk lösning ... 820

29.5 En enda myndighet bör ha huvudansvaret för en myndighetsgemensam teknisk lösning ... 823

29.6 Myndigheter som är lämpade att ansvara för en myndighetsgemensam teknisk lösning ... 824
29.6.1 Migrationsverket ... 825
29.6.2 Försäkringskassan ... 827
29.6.3 Skatteverket ... 828
29.6.4 Polismyndigheten ... 829
29.6.5 Digg ... 830
29.6.6 Sammantagen bedömning ... 834

Del 4 – Avslutande del

30 Konsekvensanalys 839

30.1 Inledning 839

30.2 Övergripande frågor 839
30.2.1 Problemet och vad våra förslag syftar till att uppnå 839
30.2.2 Effekten av att våra förslag inte genomförs och alternativa lösningar 840
30.2.3 Förenlighet med EU-rätten och Sveriges internationella åtaganden 842

30.3 Konsekvenser för enskilda 843
30.3.1 Skyddet för den personliga integriteten 848
30.3.2 Särskilt om konsekvenser för barn 849

30.4 Konsekvenser för arbetet med att förebygga och i övrigt motverka brottslighet 851

30.5 Konsekvenser för det allmänna 854
30.5.1 Verifierande myndigheter 855
30.5.2 Tekniskt ansvarig myndighet 861
30.5.3 De allmänna förvaltningsdomstolarna 864
30.5.4 Kostnadsuppskattningar 866
30.5.5 Finansiering 868
30.5.6 En myndighetsgemensam teknisk lösning bör vara avgiftsfri 869

30.6 Konsekvenser för företag 870

30.7 Övriga konsekvenser 871

31 Förslagens genomförande och ikraftträdande 873

31.1 Ikraftträdande 873

31.2 Övergångsbestämmelser 875

32 Författningskommentar 877

32.1 Förslaget till lag om biometrisk verifiering av identitet 877

32.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400) 893

Bilaga

Bilaga 1 Kommittédirektiv 2025:22 895

Sammanfattning

Inledning

I takt med en ökad digitalisering av samhället har behovet av en möjlighet till säker och tillförlitlig verifiering av identitet blivit allt tydligare. Kontakter med myndigheter sker i dag i stor utsträckning på digital väg, exempelvis vid en ansökan om en socialförsäkringsförmån, vilket har stora fördelar både för den enskilde och för myndigheterna. Ett alltmer digitaliserat samhälle har däremot också en tydlig baksida, i form av den identitetsrelaterade brottslighet som kan begås bland annat genom att använda falska identitetshandlingar eller genom att utnyttja någon annans identitet, med eller utan dennes vetskap. Enskilda kan också uppträda i multipla identiteter som har registrerats hos olika myndigheter i Sverige. Även om det inte är möjligt att närmare uppskatta omfattningen av identitetsmissbruket förekommer det på en sådan nivå att det motiverar att vidare åtgärder övervägs, inte minst då missbruket riktas mot och får följder för många myndigheter och centrala samhällsfunktioner.

Det övergripande syftet med vårt uppdrag är att skapa förutsättningar för en effektivare och säkrare process vid verifiering av identitet, som utgår från att biometriska uppgifter används. Vissa myndigheter har redan stöd för detta i olika ärendeslag. Exempelvis får Migrationsverket respektive Skatteverket använda biometriska uppgifter för att kontrollera identitet i samband med en ansökan om uppehållstillstånd respektive en anmälan om flyttning till Sverige. Fler aktörer i samhället behöver emellertid få möjlighet att genomföra sådana typer av kontroller, i syfte att motverka identitetsmissbruk. Utökade möjligheter att biometriskt verifiera identitet kan både främja myndigheters kontrollmöjligheter och utgöra ett skydd för enskilda mot att deras identitet utnyttjas i olika sammanhang.

Vårt arbete och våra förslag har utformats utifrån dessa mål.

Biometriska uppgifter behöver användas i större utsträckning

Säker verifiering av identitet innebär att en tillförlitlig koppling kan göras mellan den person som en myndighet möter och den *identitet* – vilket enligt vår definition utgörs av uppgifter om namn, födelsetid och medborgarskap – som han eller hon gör gällande, exempelvis genom att lämna uppgifter om identitet i en ansökan om sjukpenning. Med andra ord handlar det om att myndigheten ska få svar på frågan *Är personen den som han eller hon utger sig för att vara?* En sådan koppling mellan person och identitet görs i praktiken ofta genom att en företrädare för en myndighet eller någon annan aktör gör en okulär jämförelse mellan individen och en ansiktsbild som finns på en identitetshandling. En sådan jämförelse gör det möjligt att utnyttja andras identitet, exempelvis genom att så kallade look-a-likes används.

För att tillförlitligt kunna koppla ihop en individ med information om identitet som är lagrad i ett register eller i en handling, och därmed med den påstådda identiteten, behöver biometriska uppgifter kunna användas. Biometriska uppgifter är unika för varje individ och möjliggör en direkt och tillförlitlig koppling till en unik individ. När en identitet kan verifieras biometriskt blir det svårare att dölja sig bakom en falsk eller utnyttjad identitet, vilket främjar möjligheten både att följa en individ och till ansvarstagande. Våra förslag är därför utformade med utgångspunkt i användning av biometriska uppgifter.

Vi har övervägt två alternativ för säkrare verifiering av identitet

Vårt uppdrag innefattar att vi ska undersöka lämpligheten av ett system som bygger på unika identitetsnycklar i ett identitetsindex, vilket har förslagits av samverkansinitiativet MUR (Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärdssystemen). Detta har utgjort ett av de huvudalternativ för att främja säkrare verifiering av identitet som vi har analyserat. Det andra alternativet är ett system som utgår från användning av biometriska underlag som är lagrade i handlingar av olika slag. Efter att närmare ha utrett förutsättningarna för och jämfört de två alternativen har vi gått vidare med författningsförslag som utgår från det sistnämnda. Detta då vi har bedömt att ett centralt identitetsindex bland annat skulle vara mycket komplext att implementera och med-

föra ett klart större ingrepp i skyddet för den personliga integriteten än biometrisk verifiering mot handlingar. En generell möjlighet för svenska myndigheter att kontrollera biometriska uppgifter mot handlingar kan enligt vår bedömning stärka kopplingen mellan etablerad identitet och verifiering av identitet på ett ändamålsenligt och effektivt sätt.

Våra förslag tar endast sikte på biometrisk *verifiering* av identitet, det vill säga en-till-en-jämförelser av en grupp av uppgifter – däribland biometriska uppgifter – med en annan, för att avgöra om en påstådd identitet är riktig. Förslagen gör det inte möjligt för myndigheter att identifiera okända personer, genom en-till-många-jämförelser med biometriska uppgifter i ett register.

En ny lag om biometrisk verifiering av identitet

Våra förslag syftar till att en mycket bred krets av myndigheter ska kunna verifiera identitet biometriskt mot handlingar. Vi har bedömt att förslagen ska samlas i en ny *lag om biometrisk verifiering av identitet*, för att uppnå en tydlighet och förutsebarhet i regleringen och för att underlätta tillämpningen. Syftet med lagen är dels att motverka identitetsmissbruk genom att ge myndigheter möjlighet att med hjälp av biometriska uppgifter som kan tas fram ur en handling kontrollera om en påstådd identitet är riktig, dels att skydda den som kontrolleras mot att hans eller hennes personliga integritet kränks vid en sådan kontroll. Den nya lagen innehåller både bestämmelser som anger när biometrisk verifiering av identitet får användas och bestämmelser som reglerar behandlingen av personuppgifter, däribland känsliga sådana, som behöver utföras i samband med verifieringen.

Att tillförlitligt kunna kontrollera att den som en myndighet möter är den som han eller hon påstår sig vara kan utgöra en viktig komponent i att upptäcka felaktigheter, vilket kan få betydelse för det arbete med att motverka brottslighet som många myndigheter bedriver i olika omfattning. Den nya lagen ska däremot av integritetsskäl inte få användas av sådana behöriga myndigheter som avses i brottsdatalagen (2018:1177) i deras brottsbekämpande verksamhet.

En fristående, men kompletterande, utredningsåtgärd

Myndigheter kan, bland annat vid handläggningen av ett ärende, behöva vidta olika utredningsåtgärder för att kunna fatta ett beslut eller vidta en korrekt åtgärd. Biometrisk verifiering av identitet enligt den nya lagen ska ses som *en* sådan möjlig utredningsåtgärd. Den nya lagen syftar alltså till att utgöra ett fristående komplement till myndigheters befintliga utredningsåtgärder. För det fall en myndighet i annan författning har getts en uttrycklig rätt att i en viss situation biometriskt verifiera identitet mot handlingar ska den bestämmelsen tillämpas i stället för den nya lagen. Sådana andra bestämmelser, som kan innehålla särskilda begränsningar bland annat för när biometrisk verifiering får användas, finns exempelvis för Migrationsverket i utlänningslagen (2005:716) och för Skatteverket i folkbokföringslagen (1991:481). De flesta myndigheter saknar dock sådana möjligheter i dag.

Biometrisk verifiering enligt den nya lagen kan också komma att komplettera användningen av e-legitimation, som används för att få tillgång till olika nättjänster, exempelvis för att ansöka om en socialförsäkringsförmån som Försäkringskassan handlägger eller för att logga in på 1177.se, Sveriges officiella samlingsplats för information och tjänster inom hälsa och vård. Den europeiska digitala plånboken som regleras i den reviderade eIDAS-förordningen[1] ska också kunna användas i sådant syfte, det vill säga att *autentisera* en person i en nättjänst, inte att *verifiera* identiteten. Biometrisk verifiering av identitet enligt den nya lagen ska alltså inte ersätta användningen av e-legitimation, men kan komma att utgöra ett integrerat moment i en sammanhängande digital autentiserings- och verifieringsprocess, där en e-legitimation används i förstnämnda del och bäraren av den – exempelvis ett sådant statligt identitetskort som enligt förslag ska införas – används för den biometriska verifieringen. Samma fysiska handling kommer alltså att kunna användas i olika, men sammankopplade, syften.

[1] Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024.

Endast myndigheter ska få tillämpa den nya lagen

Vårt uppdrag innefattar att utvärdera om såväl statliga myndigheter som andra offentliga aktörer och privata aktörer bör omfattas av en möjlighet att använda biometriska uppgifter för en stärkt verifiering av identitet i olika sammanhang. Identitetsmissbruk riktas mot både myndigheter och privata aktörer. Den nya lag om biometrisk verifiering av identitet som vi föreslår ska av integritetsskäl dock endast få tillämpas av myndigheter. Såväl statliga som kommunala och regionala myndigheter omfattas. Riksdagen och beslutande kommunala församlingar, de organ som anges i bilagan till offentlighets- och sekretesslagen (2009:400) samt bolag, föreningar och stiftelser där kommuner eller regioner utövar ett rättsligt bestämmande inflytande omfattas däremot inte. Oaktat denna avgränsning är det alltså fråga om en mycket bred krets av myndigheter som ska få möjlighet att använda biometriska uppgifter för att verifiera identitet, jämfört med i dag.

Vem kan en begäran enligt den nya lagen omfatta?

För att den nya lagen ska kunna få ett så stort genomslag som möjligt har en utgångspunkt varit att en bred krets av personer ska kunna omfattas. I den nya lagen avgränsas personkretsen dels av vilka typer av handlingar som ska kunna användas för biometrisk verifiering, dels av att en begäran om att medverka till en sådan kontroll endast ska kunna riktas mot personer som har fyllt sex år. I praktiken kan barn, som i många avseenden saknar egen rättshandlingsförmåga, antas bli föremål för en begäran med stöd av lagen i relativt få fall.

Endast handlingar som uppfyller vissa krav i fråga om utformning och utfärdande ska få användas: hemlandspass och identitetskort som har utfärdats av behörig myndighet och som är försedda med ett lagringsmedium som innehåller biometriska underlag samt uppehållstillståndskort som har utfärdats av svenska myndigheter. Nämnda slag av handlingar kan utfärdas för såväl svenska medborgare som EES-medborgare och medborgare i tredje land. En mycket bred krets av personer som av olika anledningar vistas i eller har anknytning till Sverige kommer därmed att omfattas av den nya lagens tillämpningsområde.

Endast fysiska personer ska omfattas av den nya lagens tillämpningsområde. Det förekommer dock även identitetsmissbruk som kan hänföras till juridiska personer, genom att så kallade målvakter används för att bemanna bolagsstyrelser och som firmatecknare, och falska identiteter används i syfte att dölja vem den verkliga företrädaren i ett bolag är. Företrädare för juridiska personer kan komma att bli föremål för biometrisk verifiering enligt den nya lagen. Diplomatisk personal och de personer som tillhör en främmande stats militära styrka eller ett Natohögkvarter och som vistas i Sverige är inte undantagna från den nya lagens tillämpningsområde.

När ska biometrisk verifiering enligt den nya lagen få användas?

Den föreslagna lagen skulle ge myndigheter en *rätt* att använda biometrisk verifiering av identitet mot handlingar i vissa situationer. Det finns däremot ingen skyldighet att använda en sådan utredningsåtgärd.

Eftersom den föreslagna lagen skulle innebära ett ingrepp i skyddet för den personliga integriteten behöver det vara tydligt både för myndigheter och för enskilda när den ska få tillämpas. Samtidigt måste tillämpningsområdet vara tillräckligt brett för att uppnå de syften som lagen har. Vi har med dessa utgångspunkter utformat lagen så att myndigheter ska kunna använda biometrisk verifiering när sådan verifiering är nödvändig

1. vid handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde, eller
2. i annat fall, när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller.

Sistnämnda situation tar framför allt sikte på myndigheters faktiska verksamhet och kan användas när den enskilde befinner sig på plats hos en myndighet, exempelvis i samband med ett besök i vården, vid genomförande av högskoleprovet eller vid röstning till val. Den nya lagen kan alltså komma att användas i ett stort antal situationer då det är viktigt för myndigheter att kunna säkerställa att en person är den som han eller hon utger sig för att vara. Genom att det anges att biometrisk verifiering av identitet ska vara *nödvändig* motverkas att lagen används i situationer då det inte behövs, exempelvis när en

person är känd sedan tidigare av myndigheten och dennes identitet inte ifrågasätts. Det är som utgångspunkt upp till myndigheterna själva att avgöra när en biometrisk verifiering är nödvändig. Lagen förutsätter inte att det har kommit fram några särskilda omständigheter i det enskilda ärendet som ger anledning att anta att den enskilde försöker vilseleda myndigheten om sin identitet, utan lagen ska kunna tillämpas till exempel för att göra slumpmässiga kontroller av identitet i ärendeslag där myndigheten bedömer att det finns en risk för identitetsmissbruk.

Den enskilde kan av olika skäl anse att det inte varit nödvändigt med biometrisk verifiering i ett visst fall. Sådana invändningar kan göras gällande i samband med att han eller hon eventuellt överklagar ett beslut som fattats i ärendet eller med anledning av en genomförd identitetskontroll i annat fall.

Hur den biometriska verifieringen går till

Den föreslagna lagen ska ge myndigheter en generell rättslig möjlighet att biometriskt verifiera identitet mot handlingar. Lagen reglerar däremot inte närmare *hur* kontrollen ska genomföras i ett enskilt fall. Beroende på vilka tekniska lösningar som finns tillgängliga eller tas fram kan den biometriska verifieringen komma att genomföras såväl på plats hos en myndighet som på distans, exempelvis genom att en myndighetsgemensam mobilapplikation används.

En begäran enligt lagen innebär att den enskilde är skyldig att låta myndigheten ta biometriska underlag i form av fingeravtryck och/eller ansiktsbild, och att göra en handling tillgänglig. Det är viktigt att poängtera att det sistnämnda kravet inte innebär att den enskilde är skyldig att skaffa en viss typ av handling om han eller hon exempelvis saknar ett hemlandspass. Det kan emellertid förutsättas att den absoluta merparten av de personer som det kan finnas anledning att verifiera identitet biometriskt för också innehar en handling som kan användas, eftersom handlingarna är av sådant slag att de typiskt sett behövs för att en person ska kunna resa eller legitimera sig i många olika vardagssituationer. I fråga om uppehållstillståndskort *ska* dessa utfärdas för den som har uppehållstillstånd i Sverige. Att göra en viss handling tillgänglig kan däremot – om det

saknas en teknisk lösning för verifiering på distans – innebära att den enskilde behöver ta sig till en myndighet (personlig inställelse).

Om den som inlett det aktuella ärendet hos myndigheten inte följer en begäran om biometrisk verifiering enligt den nya lagen kan han eller hon föreläggas att medverka till att verifieringen kan genomföras. Av föreläggandet ska det framgå vad följden kan bli av att det inte följs.

Skyddet för den personliga integriteten påverkas

Den föreslagna lagen innebär att enskilda skulle kunna bli skyldiga att låta myndigheter ta fingeravtryck eller ansiktsbild i betydligt fler situationer än i dag. En bred krets av myndigheter kan komma att behandla biometriska uppgifter som tas fram ur fingeravtryck och ansiktsbilder. Detta är en skillnad mot gällande regelverk om biometrisk verifiering, som är begränsat till ett fåtal centrala myndigheter. Som vi noterat ovan kan enskilda – både i ett enskilt fall och på ett generellt plan – komma att ha invändningar mot detta, och det kan finnas en oro för att känsliga personuppgifter kan komma obehöriga till handa. Vi bedömer att det intrång i skyddet för den personliga integriteten som biometrisk verifiering enligt den nya lagen innebär motiveras av ett starkt samhällsintresse, nämligen att motverka identitetsmissbruk, och att intrånget är proportionerligt. Vi vill särskilt understryka att den nya lagen inte endast ger myndigheter utökade kontrollverktyg, utan också utgör en form av skyddslagstiftning som motverkar att någons identitet utnyttjas utan hans eller hennes vetskap.

Risken för att känsliga personuppgifter sprids till obehöriga motverkas av våra förslag på flera sätt. För det första ska endast myndigheter få tillämpa den nya lagen. För det andra anges i lagen att fingeravtryck och ansiktsbilder samt de biometriska uppgifter som har tagits fram och använts vid biometrisk verifiering omedelbart ska förstöras efter att kontrollen har genomförts. Uppgifterna får alltså inte lagras i något register eller användas för något annat ändamål än vad som anges i lagen. För det tredje föreslår vi att nämnda typer av uppgifter ska omfattas av absolut sekretess, genom att en ny bestämmelse införs i offentlighets- och sekretesslagen.

Sammantaget bedömer vi att våra förslag innehåller ett tillfredsställande skydd för den personliga integriteten.

Konsekvenser

En generell möjlighet för myndigheter att verifiera identitet säkrare, i enlighet med våra förslag, kan som vi ser det få stor betydelse för att minska förekomsten av utnyttjande av identiteter, och kan främja korrekt ärendehandläggning och beslutsfattande. Den nya lagen kan därför ha positiva effekter på myndigheters arbete med att förebygga och i övrigt motverka brottslighet, såväl direkt som indirekt. Det faktiska genomslaget är visserligen svårt att förutse och är i viss mån beroende på hur det rättsliga stödet som våra förslag innebär tekniskt implementeras i praktiken. Vi bedömer dock att redan *möjligheten* för myndigheter att i stor omfattning kunna använda biometrisk verifiering av identitet kan vara handlingsdirigerande och få ett avskräckande och avhållande syfte. Exempelvis kan ett vanligt förekommande upplägg, innebärande att en e-legitimation för en person – som endast tillfälligt har vistats i Sverige i syfte att etablera en identitet som används som ”målvakt” – därefter används av andra, bli betydligt mindre attraktivt.

Vissa kostnader för det allmänna

En rättslig möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar med stöd av våra förslag skulle inte i sig medföra några direkta kostnader för det allmänna. Det är i stället primärt utveckling och drift av tekniska system som möjliggör biometrisk verifiering som i praktiken kommer att driva kostnader, och då i första hand ett eventuellt myndighetsgemensamt system. En sådan teknisk lösning är dock av stor betydelse för att förslagen ska kunna få ett genomslag i praktiken, genom att den skulle göra det möjligt att genomföra biometrisk verifiering av identitet på distans. Oavsett vilken teknisk lösning som används kan de myndigheter som vill använda den nya lagen behöva investera i vissa tekniska system. Myndigheterna kan också, utifrån sin verksamhet, behöva göra dataanalyser och urval för att kunna använda biometrisk verifiering på ett ändamålsenligt och effektivt sett. Sådana kontroller kan inne-

bära ett ändrat arbetssätt och behov av såväl interna utbildningsinsatser som informationsinsatser till allmänheten. Ökade kostnader för detta kan i första hand förväntas under en övergångsperiod. För myndigheter med omfattande verksamhet och ett stort behov av biometrisk verifiering kan det antas att dessa initiala kostnader inte kommer att rymmas inom befintliga anslag och att anslagen därmed behöver höjas. För mindre myndigheter, som får möjlighet att ansluta sig till en myndighetsgemensam teknisk lösning, bör såväl de initiala kostnaderna som de löpande däremot kunna täckas av befintliga anslag.

En myndighet som får i uppdrag att tekniskt ansvara för en myndighetsgemensam lösning för biometrisk verifiering av identitet med stöd av den nya lagen kommer att behöva ökade anslag både initialt och löpande, för att täcka kostnader relaterade till utveckling av tekniska system i form av en mobilapplikation, ett backend-system och gränssnitt mot verifierande myndigheters system, till förvaltning och drift, till en kundportal och support samt till informationsinsatser.

Våra förslag bedöms både ha en avskräckande effekt och främja att faktiskt identitetsmissbruk upptäcks. Det kan i sin tur förväntas leda bland annat till att brott mot välfärdssystemen upptäcks i större utsträckning, vilket skulle innebära minskade kostnader för det allmänna.

Konsekvenser för enskilda

Som vi nämnt ovan ska den nya lagen ses inte bara som en kontrollmöjlighet för det allmänna, utan som en form av skyddslagstiftning för enskilda mot att deras identitet utnyttjas av andra utan deras vetskap, vilket är ett ökande problem i ett alltmer digitaliserat samhälle. De konsekvenser för skyddet för den personliga integriteten som vi redogjort för ovan måste ses mot bakgrund av detta.

Vi bedömer att våra förslag – utöver eventuella kostnader för resor och förlorad arbetsinkomst i samband med att en biometrisk verifiering med stöd av den nya lagen genomförs vid personlig inställelse – inte medför några kostnader för enskilda. Den nya lagen innebär inte att enskilda är skyldiga att inneha eller skaffa sådana handlingar som kan användas för den biometriska verifieringen av identitet.

Våra förslag omfattar även barn som har fyllt sex år. Konsekvenserna av våra förslag för barn som ett kollektiv kan emellertid antas bli mycket begränsade. Vi bedömer att upptagning av biometriska underlag med stöd av lagen för ett barn, när det trots allt kan bli aktuellt, inte kan antas innebära ett större integritetsintrång än för en vuxen.

Summary

Introduction

With the increasing digitalisation of society, the need for a means to safely and reliably verify identity has become increasingly evident. Interactions with public authorities are now largely conducted digitally, for instance when applying for social security benefits, which offers significant advantages for both the individual and the authorities. However, an increasingly digitised society also presents a downside in the form of identity-related crime, which can be committed, for example, by using falsified identity documents or by exploiting someone else's identity, with or without their knowledge. Individuals can also use multiple identities that have been registered with various public authorities in Sweden. Although it is not possible to fully assess the extent of identity abuse, it occurs at a level that warrants consideration of further measures, particularly as the abuse targets and has consequences for numerous public authorities and central societal functions.

The overarching objective of our remit is to create conditions for a more effective and secure process for verifying identity, using biometric data. Certain public authorities already have support for this in various case types. For example, the Swedish Migration Agency and the Swedish Tax Agency may use biometric data to verify identity in connection with an application for a residence permit or when relocating to Sweden. Nevertheless, more actors in society need to be granted the opportunity to carry out such controls, in order to counteract identity abuse. Expanded possibilities for biometric identity verification can both promote the control capabilities of authorities and serve as a protection for individuals against their identities being exploited in various contexts. Our work and proposals have been formulated based on these objectives.

Biometric data needs to be used more extensively

Secure identity verification involves establishing a reliable link between the person encountered by an authority and the identity – which, according to our definition, consists of name, date of birth, and citizenship – that person claims, for example, by submitting such information in an application for a social insurance benefit. In other words, it is about the public authority getting an answer to the question: "Is the person the one they claim to be?" Such a link between the person and the identity is often practically established when a representative of a public authority conducts an ocular comparison between the individual and a facial image on an identity document. Such a comparison allows for the exploitation of others' identities, for instance through so-called look-a-likes.

In order to reliably link an individual with identity information stored in a register or document, and thereby with the alleged identity, biometric data must be able to be used. Biometric data is unique to each individual and enables a direct and reliable link to a unique individual. When an identity can be verified biometrically, it becomes more difficult to conceal oneself behind a false or exploited identity, which promotes both the ability to track an individual and hold them accountable. Our proposals are therefore designed based on the use of biometric data.

We have considered two alternatives for more secure verification of identity

Our remit includes investigating the suitability of a system based on unique identity keys stored in an identity index, as proposed by the MUR initiative, Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärdssystemen (Payment and Act Enforcement Authorities' Resistance to the Abuse and Breach of Sweden's Welfare Systems). This has constituted one of the main alternatives for promoting more secure identity verification that we have analysed. The second alternative is a system based on the use of biometric information stored in various types of documents. After further examining the prerequisites for and comparing the two alternatives, we have proceeded with legislative proposals based on the latter. This is based on our assessment that a central

identity index would be very complex to implement and would entail a significantly greater interference with the protection of personal integrity than biometric verification against documents. A general possibility for Swedish authorities to validate biometric data against documents can, in our assessment, strengthen the link between an established identity and identity verification, in a purposeful and effective manner.

Our proposals are solely aimed at biometric *verification* of identity, meaning a one-to-one comparison of one set of data – including biometric data – with another, in order to determine whether an alleged identity is genuine. The proposals do not allow authorities to identify unknown persons through one-to-many comparisons of biometric data stored in a database.

A new Biometric Identity Verification Act

Our proposals aim for a broad range of public authorities to be able to verify identity biometrically against documents. We have assessed that the proposals should be collected in a new Biometric Identity Verification Act to achieve clarity and predictability in the regulation and to facilitate the application. The purpose of the new Act is twofold: firstly, to counteract identity abuse by giving public authorities the opportunity to use biometric data extracted from a document to check whether an alleged identity is correct, and secondly, to protect the person being checked against the infringement of their personal integrity, during such a check. The new Act will contain provisions specifying when biometric identity verification may be used and provisions regulating the processing of personal data, including sensitive data, that must be carried out in connection with the verification.

To be able to reliably verify that a person that a public authority encounters is who he or she claims to be is an important component in detecting inaccuracies, which can be significant for the work of combating crime that many authorities undertake to varying extents. However, the new Act cannot be used by such competent authorities as referred to in the Criminal Data Act (2018:1177) in their law enforcement activities, due to privacy considerations.

An independent, yet complementary, investigative measure

Public authorities may need to take various investigative measures, for instance when handling a case, in order to make a decision, or take the correct action. Biometric identity verification according to the new Act should be considered as such an investigative measure. The new Act thus aims to constitute an independent, complementary, measure to the public authorities' existing investigative measures. In cases where another piece of legislation has granted an explicit right to biometric identity verification against documents in a certain situation, that provision shall apply instead of the new Act. Such other provisions, which may contain specific limitations, including for when biometric verification may be used, are found, for example, in the Aliens Act (2005:716) for the Swedish Migration Agency and in the Population Registration Act (1991:481) for the Swedish Tax Agency. Most public authorities, however, lack such possibilities today.

Biometric verification under the new Act may also complement the use of electronic identification (eID), which is used to access various online services, such as applying for a social security benefit handled by the Swedish Social Insurance Agency or logging into 1177.se, Sweden's official platform for information and services in healthcare. The European digital wallet regulated by the revised eIDAS Regulation[1] can also be used for such purposes, that is, to *authenticate* a person in an online service, not to *verify* the identity. Biometric identity verification under the new Act does therefore not replace the use of electronic identification. However, it may become an integrated element in a coherent digital authentication and verification process, where an eID is used in the former part and the physical bearer of it – for example, such a government identity card that has been proposed – is used for the biometric verification. The same physical document can thus be used for different, yet interconnected, purposes.

[1] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024.

Only public authorities may apply the new Act

Our remit includes evaluating whether both government agencies and other public and private actors should be covered by a possibility to use biometric data for strengthened identity verification in various contexts. Identity abuse targets both public authorities and private entities. The new Act on biometric identity verification that we propose is, however, only applicable to public authorities, due to privacy considerations. National, municipal, and regional public authorities are covered. The Riksdag and decision-making municipal councils, the bodies specified in the appendix to the Public Access to Information and Secrecy Act (2009:400), as well as companies, associations, and foundations where municipalities or regions exercise a legally controlling influence are not covered. Despite this delimitation, a very broad circle of public authorities will be granted the opportunity to use biometric data to verify identity, in contrast to today.

Who can a request under the new Act target?

For the new Act to have the greatest impact, the starting point has been that a broad circle of persons should be covered. The new Act delimits the circle of individuals partly by the types of documents that may be used for biometric verification, and partly by the fact that a request to participate in such a check may only be directed towards persons who have reached the age of six years. In practice, children, who lack legal capacity in many respects, are to be presumed to be subject to a request under the Act in relatively few cases.

Only documents that meet certain requirements regarding design and issuance shall be used: passports and identity cards issued by competent authorities and which are equipped with a storage medium containing biometric information, as well as residence permit cards issued by Swedish authorities. Such types of documents may be issued for Swedish citizens as well as EEA citizens and third-country nationals. A very broad circle of persons who reside in or have ties to Sweden for various reasons will thus be covered by the scope of application of the new Act.

Only physical persons shall be covered by the scope of application of the new Act. However, identity abuse that can be attributed to

legal persons may also occur, through the use of so-called straw men to staff a board of directors and as company signatories, and false identities may be used to conceal who the true representative of a company is. Representatives of legal persons may be subject to biometric verification under the new Act. Diplomatic personnel and individuals belonging to a foreign state's military force or a NATO headquarters who reside in Sweden are not exempt from the scope of application of the new Act.

When can biometric verification under the new Act be used?

The proposed Act would grant public authorities a right to use biometric identity verification using documents in certain situations. There is, however, no obligation to use such an investigative measure.

Since the proposed Act would involve an interference with the protection of personal integrity, it must be clear both for public authorities and individuals when it should be applied. At the same time, the scope of application must be broad enough to achieve the purposes of the Act. We have designed the Act with these premises so that public authorities may use biometric verification when such verification is necessary

1. in the handling of a case covered by the scope of application of the Administrative Procedure Act (2017:900), or
2. in other situations, when the authority, within the scope of its operations, conducts identity checks.

The latter situation primarily targets the actual activities of public authorities and can be used when the individual is present at an authority, for example, in connection with a medical visit, when taking the Swedish Scholastic Aptitude Test (högskoleprovet) or when voting. The new Act may therefore be used in a large number of situations where it is important for public authorities to ensure that a person is who they claim to be. Biometric identity verification must be *necessary*, which is intended to prevent the Act from being used in situations where it is not needed, for example, when a person is already known to the public authority and their identity is not questioned. It is up to the authorities to decide when a biometric verification is necessary. The Act does not presuppose that

any particular circumstances in the individual case has arisen that gives reason to assume that the individual is attempting to mislead the public authority about their identity; rather, the Act can be used, for example, to conduct random identity checks in case types where the authority assesses there is a risk of identity abuse.

The individual may, for various reasons, consider that biometric verification was not necessary in a certain situation. Such objecttions may be raised when he or she, possibly, appeals a decision made in the case or in connection with an identity check that has been conducted in another situation.

How the biometric verification is conducted

The proposed Act would grant public authorities a general legal right to biometrically verify identity against documents. The Act, however, does not regulate in detail how the check should be conducted in a specific case. Depending on the technical solutions available, the biometric verification may be carried out either on-site at an authority or remotely, for example, by using a shared mobile application, developed by a central public authority.

A request under the Act implies that the individual is obliged to allow the public authority to capture biometric data in the form of fingerprints and/or facial images, and to make a document available. It is important to emphasize that the latter requirement does not mean that the individual is obliged to obtain a certain type of document if they, for example, lack a passport. However, it can be presumed that the absolute majority of the persons for whom there is reason to verify identity biometrically also possess a document that can be used, since such documents are typically required for a person to travel or show proof of identify in many different daily situations. Regarding residence permit cards, these are issued for anyone who is granted a residence permit in Sweden. Making a certain type of document available may, however, imply that the individual needs to visit the office of a public authority (personal appearance) if there is no technical solution for remote verification.

If the person who initiated the relevant case with the public authority does not comply with a request for biometric verification under the new Act, they can be ordered to cooperate so that the verifica-

tion can be carried out. The injunction shall specify what the consequence will be if it is not complied with.

The protection of personal integrity is affected

The proposed Act implies that individuals may be obliged to allow public authorities to capture fingerprints or facial images in significantly more situations than today. A broad range of authorities may have to process the biometric data extracted from fingerprints and facial images. This differs from current regulations on biometric verification, which are limited to a few central public authorities. As we have noted above, individuals – both in a specific case and in a general sense – may object to this, and there may be a concern that sensitive personal data may fall into the wrong hands. Our assessment is that the interference with the protection of personal integrity that biometric verification under the new Act entails is justified by a strong societal interest, namely, to counteract identity abuse, and that the interference is proportionate. We wish to emphasize that the new Act not only grants authorities expanded control tools but also constitutes a form of protective legislation that counteracts the exploitation of someone's identity without their knowledge.

The risk of sensitive personal data spreading to unauthorized parties is counteracted by our proposals in several ways. Firstly, only public authorities will be entitled to apply the new Act. Secondly, the Act stipulates that fingerprints and facial images, as well as the biometric data obtained from them and used in biometric verification, shall be destroyed immediately after the check has been completed. The data can therefore not be stored in any register or used for any purpose other than what is stated in the new Act. Thirdly, we propose that such types of data shall be subject to absolute secrecy by introducing a new provision in the Public Access to Information and Secrecy Act.

In summary, our proposals contain satisfactory protection for personal integrity.

Consequences

A general possibility for public authorities to verify identity more securely, in accordance with our proposals, may have great significance in reducing the occurrence of identity exploitation and may promote correct case handling and decision-making. The new Act can therefore have positive effects on public authorities' work to prevent and otherwise counteract crime, both directly and indirectly. The actual impact is admittedly difficult to predict and is to some extent dependent on how the legal support that our proposals entail is technically implemented in practice. We nevertheless assess that the very possibility for public authorities to use biometric identity verification may to a large extent influence individuals' behaviour and have a deterrent and restraining effect. For example, a common setup, involving using an eID issued to a person who has only temporarily resided in Sweden to establish an identity to be used as a "straw man", would be significantly less attractive.

Certain costs for public authorities

A legal possibility for authorities to verify identity biometrically using documents, using our proposals, would not in itself entail any direct costs for public authorities. It is rather the development and operation of technical systems that enable biometric verification which will drive costs in practice, and primarily a potential shared technical system that can be used by all public authorities. Such a technical solution is, however, of great importance for the proposals to gain traction in practice, by making it possible to carry out biometric identity verification remotely. Regardless of which technical solution is used, the public authorities wishing to use the new Act will need to invest in certain technical systems. Authorities may also need to conduct data analyses and selections, based on their operations, in order to use biometric verification in a purposeful and effective manner. Such checks may involve a changed workflow and a need for both internal training efforts and information efforts directed towards the public. Increased costs for this are expected primarily during a transition period. For authorities with extensive operations and a great need for biometric verification, we presume that these initial costs will not be covered within existing appropriations and

that the appropriations will therefore need to be increased. For smaller authorities, which are granted the opportunity to join and use a shared technical solution, both the initial costs and the ongoing ones should, presumably, be covered by existing appropriations.

A public authority that is assigned a technical responsibility for managing a shared solution for biometric identity verification using the new Act will need increased appropriations, both initially and continuously, to cover costs related to the development of technical systems in the form of a mobile application, a backend system and an interface to verifying authorities' systems, administration and operation, customer portal and support, as well as information efforts.

We assume that our proposals may have a deterrent effect and can promote the actual detection of identity abuse. This may, in turn, be expected to lead to the detection of violations of welfare systems to a greater extent, which would imply reduced costs for the public.

Consequences for individuals

As mentioned above, the new Act should not only be seen as a control possibility for the public but as a form of protective legislation for individuals against their identity being exploited by others without their knowledge, which is a growing problem in an increasingly digitised society. The consequences for the protection of personal integrity that we have described above must be viewed in light of this.

Our assessment is that our proposals – apart from potential costs for travel and lost income in connection with a biometric verification in accordance with the new Act which is conducted through personal appearance – do not entail any costs for individuals. The new Act does not imply that individuals are obliged to possess or obtain such documents that can be used for the biometric verification of identity.

Our proposals also cover children who have reached the age of six years. The consequences of our proposals for children as a collective may, however, be considered to be very limited. We assess that the capture of biometric data in accordance with the Act for a child, when it may prove relevant, cannot be presumed to entail a greater infringement of integrity than for an adult.

1 Författningsförslag

1.1 Förslag till lag om biometrisk verifiering av identitet

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens syfte

1 § Syftet med denna lag är att motverka identitetsmissbruk genom att ge myndigheter möjlighet att med hjälp av biometriska uppgifter som kan tas fram ur en handling kontrollera om en påstådd identitet är riktig och att skydda den som kontrolleras mot att hans eller hennes personliga integritet kränks vid en sådan kontroll.

Förhållande till annan reglering

2 § Denna lag kompletterar 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), här benämnd dataskyddsförordningen.

Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller av föreskrifter som har meddelats i anslutning till lagen.

3 § Om en annan lag eller förordning innehåller en bestämmelse som ger en myndighet uttrycklig rätt att kontrollera om en persons fingeravtryck eller ansiktsbild motsvarar dem som finns i en handling ska den bestämmelsen tillämpas.

Undantag för brottsbekämpande verksamhet

4 § En biometrisk verifiering får inte genomföras med stöd av lagen i verksamhet som en sådan behörig myndighet som avses i brottsdatalagen (2018:1177) utför i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Definitioner

5 § I denna lag avses med

1. *identitet:* uppgifter om namn, födelsetid och medborgarskap,
2. *biometriska uppgifter:* personuppgifter som genom en särskild teknisk behandling har tagits fram ur fingeravtryck eller ansiktsbild, i syfte att verifiera en persons identitet,
3. *biometrisk verifiering av identitet:* en-till-en-jämförelse av en grupp av uppgifter, däribland biometriska uppgifter, med en annan för att fastställa om en påstådd identitet är riktig,
4. *myndighet:* statliga och kommunala organ, med undantag för beslutande politiska församlingar.

2 kap. Biometrisk verifiering av identitet mot handlingar

Typer av handlingar som får användas

1 § Hemlandspass och identitetskort som har utfärdats av behörig myndighet och som har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade får användas för att biometriskt verifiera innehavarens identitet med stöd av 2 §. Även upphållstillståndskort som har utfärdats av svenska myndigheter får användas för sådan verifiering.

När biometrisk verifiering av identitet får användas

2 § Den som har fyllt sex år och innehar en sådan handling som anges i 1 § ska på begäran av en myndighet göra handlingen tillgänglig samt låta myndigheten ta fingeravtryck och ansiktsbild för kontroll av att de motsvarar dem som finns i eller på handlingen, om en biometrisk verifiering av innehavarens identitet är nödvändig

1. vid handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde, eller

2. i annat fall, när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller.

När en kontroll enligt första stycket har genomförts ska fingeravtryck och ansiktsbilder samt de biometriska uppgifter som har tagits fram omedelbart förstöras.

Föreläggande om att medverka

3 § Om det inte har kommit fram omständigheter som talar mot det får en myndighet förelägga den som inte har följt en begäran enligt 2 § första stycket 1, och som har inlett ärendet, att göra en handling tillgänglig och låta myndigheten ta fingeravtryck och ansiktsbild, för att en biometrisk verifiering av identitet ska kunna genomföras.

I föreläggandet ska det anges vad följden av att det inte följs kan bli.

Överklagande

4 § En begäran enligt 2 § första stycket 1 och ett föreläggande enligt 3 § får överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs.

Rätt att meddela föreskrifter

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om tillämpningen av denna lag.

3 kap. Personuppgiftsbehandling

Tillämpningsområde

1 § Detta kapitel tillämpas vid behandling av personuppgifter som utförs i syfte att biometriskt verifiera identitet med stöd av lagen.

Ändamål och tillgång till personuppgifter

2 § Personuppgifter får behandlas endast för att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras. Detta gäller även sådana personuppgifter som avses i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter).

3 § Tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Personuppgiftsansvar

4 § Den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras med stöd av 2 kap. 2 § är personuppgiftsansvarig för den behandling av personuppgifter som utförs med anledning av det.

Rätt att göra invändningar

5 § Artikel 21.1 i dataskyddsförordningen om rätten att göra invändningar gäller inte vid sådan behandling av personuppgifter som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Denna lag träder i kraft den 1 januari 2028.

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att det ska införas en ny paragraf, 40 kap. 5 a §, och närmast före den en ny rubrik med följande lydelse,

dels att 40 kap. 8 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	40 kap.
	Biometrisk verifiering
	5 a §
	Sekretess gäller för uppgift i form av fingeravtryck eller ansiktsbild som tagits upp med stöd av lagen (202X:000) om biometrisk verifiering av identitet, och biometrisk uppgift som har tagits fram ur fingeravtrycket eller ansiktsbilden.
	8 §
Den tystnadsplikt som följer av 1, 2, 4, 5, 7 d och 7 g §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.	Den tystnadsplikt som följer av 1, 2, 4, 5, *5 a*, 7 d och 7 g §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Denna lag träder i kraft den 1 januari 2028.

2 Utredningens uppdrag och arbete samt betänkandets disposition

2.1 Våra direktiv

Regeringen beslutade den 6 mars 2025 att ge en särskild utredare i uppdrag att lämna förslag som stärker kopplingen mellan fastställd grundidentitet och verifiering av identitet (dir. 2025:22). Syftet med uppdraget är att skapa en effektivare och säkrare process vid verifiering av identitet som utgår från biometriska uppgifter. Förslagen ska bidra till en effektiv, tillförlitlig och ändamålsenlig identitetsförvaltning i Sverige. Kommittédirektiven finns bifogade till betänkandet i bilaga 1.

Uppdraget innebär att vi ska lämna förslag som stärker kopplingen mellan grundidentitet och verifiering av identitet med grund i biometriska uppgifter och i det sammanhanget undersöka lämpligheten med ett system med en unik identitetsnyckel. Vidare ska vi undersöka vilket eller vilka tekniska stöd som behövs för att stärka kopplingen mellan grundidentitet och verifiering av identitet samt analysera vilka risker som behandlingen av personuppgifter kan innebära och göra nödvändiga säkerhetsanalyser. Vi ska även lämna förslag om vilken eller vilka myndigheter som ska ansvara för de uppgifter som behöver utföras och vid behov omhänderta förslag som identifierats i pågående myndighetsuppdrag. Vi ska också lämna nödvändiga författningsförslag.

2.2 Utgångspunkter och avgränsningar

I våra direktiv anges att förslag som lämnats i tidigare och pågående utredningar om utökade möjligheter till insamling och lagring av biometriska uppgifter ska vara utgångspunkt för analysen samt att det kan finnas behov av att ta ställning till och utreda om gällande rätt och föreslagna ändringar är tillräckliga för ändamålet verifiering av identitet. I vårt arbete har utgångspunkten varit att relevanta författningsförslag som lämnats av andra utredningar och som bereds inom Regeringskansliet kommer att leda till lagstiftning, även om det sker först efter att vi redovisat vårt betänkande. Vi har dock inte utvärderat lämnade förslag som sådana, utan fokuserat på om gällande rätt och föreslagna ändringar är tillräckliga för ändamålet att stärka verifiering av identitet, i enlighet med våra direktiv. En följd av det är till exempel att vi inte kommer att överväga nya former av fysiska eller digitala identitetshandlingar eller annan utformning av befintliga eller föreslagna handlingar. I de avseenden vi anser att redan lämnade förslag är relevanta kommer vi att redogöra för förslagen i aktuella kapitel eller avsnitt; exempelvis utgår vi från att vissa identitetshandlingar – ett statligt identitetskort – kommer att införas och ersätta vissa befintliga identitetshandlingar.

Vidare anser vi att uppdraget bör begränsas till en analys av de rättsliga förutsättningarna för säkrare verifiering av identitet. Åtgärder för att till exempel öka myndigheters kompetens, förbättra myndighetsinterna rutiner och processer samt liknande frågor – som inte bör regleras i författning – ligger enligt vår mening utanför uppdraget (se även avsnitt 10.2.1).

I de avseenden vi gör ytterligare avgränsningar, vid överväganden i olika relevanta delfrågor, redogör vi för det i respektive kapitel eller avsnitt. Som exempel kan nämnas vår utvärdering av vilket eller vilka tekniska stöd som behövs för att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet, där vi tagit ställning till vilka huvudsakliga tekniska lösningsalternativ som vi anser bör övervägas, och vilka tekniska funktioner som på ett mer övergripande plan kan komma att behövas för en säkrare verifieringsprocess i enlighet med våra förslag, men bedömt att vi inom ramen för vårt uppdrag inte har möjlighet att lämna mer detaljerade förslag om hur de tekniska systemen närmare bör eller ska utformas (se kapitel 27).

2.3 Vårt arbete

Arbetet i utredningen påbörjades i mars 2025 och har bedrivits i nära samarbete med de experter som regeringen förordnat. Utredningen har haft sex sammanträden, varav ett tvådagarssammanträde i september 2025 och ett slutinternat på två dagar i juni 2026. Utöver sammanträdena har vi haft kontakt med experterna löpande för att fördjupa oss i specifika frågor.

I juni 2025 hade vi enskilda möten med representanter för Skatteverket och för Polismyndigheten, där våra experter från Skatteverket respektive experten från Polismyndigheten deltog. Vi hade också ett möte med Migrationsverkets expert i utredningen i juni 2025. Mötena syftade till att få en bättre uppfattning om hur dessa myndigheter arbetar med verifiering av identitet i dag, i de olika ärendeslag som myndigheterna handlägger, och vilka behov myndigheterna ser i detta avseende i sina verksamheter framöver.

Under hösten 2025 genomförde vi en enkätundersökning som skickades till sammanlagt drygt 110 mottagare: privata aktörer, statliga affärsverk, kommuner, statliga förvaltningsmyndigheter, vissa svenska utlandsmyndigheter, domstolar och Domstolsverket. Enkäten innehåll frågor om bland annat identitetskontroller, behov och utökad användning av biometri. Vi fick in cirka 50 svar. I relevanta delar har dessa svar beaktats i betänkandetexten och redovisas därför inte särskilt.

I september 2025 hade vi ett möte med Integritetsskyddsmyndigheten för att diskutera frågor om dataskydd och personlig integritet. I november 2025 träffade vi Serviceavdelningen hos Polismyndigheten, som ville informera om myndighetens syn på vårt uppdrag och på behoven inom den statliga identitetsförvaltningen. Samma månad träffade vi också Finansiell ID-Teknik BID AB (BankID), för att ta del av deras erfarenheter avseende användningen av BankID och deras tankar kring framtida behov, framför allt kopplat till biometri.

2.4 Betänkandets disposition

Betänkandet är uppdelat i fyra delar; en allmän del med utgångspunkter för våra fortsatta överväganden, en del där två huvudalternativ för att stärka kopplingen mellan etablerad grundidentitet och verifier-

ing av identitet utreds, en del med förslag på reglering av ett system för biometrisk verifiering av identitet mot handlingar samt en avslutande del.

I den första allmänna delen redogör vi för olika centrala begrepp som används i betänkandet (kapitel 3 och 4) samt går översiktligt igenom tillämpliga regelverk för dataskydd och grundläggande rättigheter (kapitel 5). I den allmänna delen redogör vi även för ärenden hos Skatteverket, Migrationsverket och Polismyndigheten där en grundidentitet kan behöva etableras (kapitel 6) samt för hur dessa myndigheter genom olika utredningsåtgärder kan verifiera identitet för personer som vistas eller vill vistas i Sverige, och vid utfärdande av olika svenska rese- och identitetshandlingar (kapitel 7). Den allmänna delen innehåller också en redogörelse för Skatteverkets, Migrationsverkets och Polismyndighetens registrering av identitetsuppgifter och andra uppgifter i befintliga register (kapitel 8) och ett kapitel med en översikt av olika typer av identitetsmissbruk samt orsaker till samt konsekvenser och omfattningen av identitetsmissbruk (kapitel 9). Sist i den allmänna delen utvärderar vi tänkbara åtgärder för säkrare verifiering av identitet och kommer fram till att två huvudalternativ bör övervägas och utredas ytterligare (kapitel 10).

I del 2 utvärderar vi utformningen av de två huvudalternativen: ett system med ett identitetsindex som bygger på unika identitetsnycklar, respektive en möjlighet att biometriskt verifiera identitet mot handlingar (kapitel 11–22). I detta avseende tar vi bland annat ställning till vilken personkrets som bör omfattas, genom att bedöma under vilka förutsättningar en person bör registreras i ett identitetsindex (kapitel 13) respektive mot vilka handlingar en biometrisk verifiering bör kunna göras (kapitel 19). Vi tar också ställning till vilka aktörer som bör kunna verifiera identitet på de olika sätten, under vilka förutsättningar som sådana kontroller bör kunna användas samt respektive alternativs förenlighet med dataskyddsförordningen och grundläggande rättigheter (kapitel 16, 17 och 21). Syftet med utvärderingen av hur de båda alternativen skulle kunna utformas är att konkretisera dessa, för att kunna analysera för- och nackdelar med respektive alternativ. För det fall lagstiftaren skulle vilja gå vidare med ett system som bygger på ett identitetsindex kan våra överväganden i framför allt kapitel 11–18 men även kapitel 21 utgöra nödvändigt beredningsunderlag för eventuella författningsförslag, eller den ytterligare utredning av ett sådant system som då kan behövas. I del 2 är

fokus alltså inledningsvis en förutsättningslös prövning av olika delfrågor som aktualiseras för det fall utredningen skulle föreslå ett system med ett identitetsindex respektive en möjlighet att verifiera identitet biometriskt mot handlingar. Därefter jämför vi de två huvudalternativen, vilket resulterar i bedömningen att utredningen bör gå vidare med en möjlighet att biometriskt verifiera identitet mot handlingar (kapitel 22).

I del 3 preciserar vi utformningen av ett system för och en reglering avseende biometrisk verifiering av identitet mot handlingar och tar ställning till ytterligare frågor av betydelse för ett system som möjliggör sådan verifiering för myndigheter – däribland frågor om dataskydd och sekretess – och lämnar nödvändiga författningsförslag (kapitel 23–25). Del 3 innehåller även en analys av processuella och tekniska frågor (kapitel 26 och 27) samt de frågor om informations- och cybersäkerhet samt säkerhetsskydd som kan aktualiseras med anledning av våra förslag (kapitel 28). I kapitel 29 utvärderar vi vilken eller vilka myndigheter som bör ges ansvar för en eventuell myndighetsgemensam teknisk lösning för att biometriskt verifiera identitet enligt våra förslag.

Avslutningsvis innehåller del 4 en konsekvensanalys (kapitel 30), överväganden avseende genomförande och ikraftträdande av förslagen (kapitel 31) samt författningskommentar (kapitel 32).

DEL 1

Allmänna utgångspunkter

3 Identitet

3.1 Inledning

Vårt övergripande uppdrag är att lämna förslag som stärker kopplingen mellan vad som i olika sammanhang benämns grundidentitet och verifiering av denna. Syftet är att främja en identitetsförvaltning som är tillförlitlig och solid, vilket i sin tur främjar möjligheten för myndigheter och andra aktörer att i olika sammanhang bekräfta vem individen man möter är. En tillförlitlig och solid identitetsförvaltning är av vikt för att motverka och förebygga brott som bygger på användning av felaktiga och falska identiteter, eller utnyttjande av andras identiteter (se kapitel 9). Vi kan konstatera att flera olika begrepp som rör identitet förekommer i olika sammanhang. Det finns därför anledning att inledningsvis ta upp vissa centrala begrepp kring identitet som vi använder i betänkandet.

3.2 Identitetsbegreppet

Vår definition

Med begreppet *identitet* avses i detta betänkande uppgifter om en individs namn, födelsetid och medborgarskap.

Identitetsbegreppet är av central betydelse på utlänningsrättens område men även vid exempelvis en ansökan om svenskt medborgarskap, vid tilldelning av samordningsnummer och när ett personnummer fastställs. Det saknas emellertid såväl en legaldefinition som vägledande förarbetsuttalanden om hur begreppets närmare innebörd generellt sett ska tolkas. En tolkning av vad som avses med identitet har i stället växt fram i praxis, främst på utlänningsrättens område,

och identitet anses då som utgångspunkt omfatta personens namn, födelsetid och medborgarskap (se MIG 2010:17, MIG 2023:7 och MIG 2024:6). Av den ändring i 28 § folkbokföringslagen (1991:481) som trädde i kraft den 1 september 2022 framgår att en anmälan om inflyttning ska innehålla bland annat dessa uppgifter. I förarbetena till ändringen gjordes bedömningen att begreppet identitet i folkbokföringslagen innefattar uppgift om namn, födelsetid och medborgarskap[1]. I 2017 års ID-kortsutredning förordades däremot, i det sammanhang som var aktuellt, att begreppet identitet i huvudsak avser en persons namn och person- eller samordningsnummer, men att även andra uppgifter om en person, såsom födelsetid, medborgarskap och bostadsadress kan hänföras till identitetsbegreppet.[2]

Att en individs identitet, utifrån den definition av begreppet som redogjorts för ovan, är styrkt innebär inte att det också är fråga om en unik identitet. Som anfördes i betänkandet *Om folkbokföring, samordningsnummer och identitetsnummer* kan det knappast sägas att en identitet är styrkt utan att de enskilda personuppgifterna som utgör en identitet kan knytas till en viss person; i annat fall är det snarare de enskilda uppgifterna som kan anses styrkta.[3] Flera individer kan alltså ha samma identitet, utan att någon av identiteterna är felaktig eller falsk. För att kunna främja säkrare sätt att verifiera identitet krävs därför ytterligare information som kan koppla en påstådd identitet till en viss, unik, individ och andra uppgifter som han eller hon har lämnat om identiteten. Biometriska uppgifter är ett sätt (se avsnitt 7.4). Sådana uppgifter kan också användas för att identifiera en individ när identiteten inte kan verifieras (se avsnitt 7.3), till exempel i samband med en inre utlänningskontroll. Vi kan notera att i artikel 3.22.a i in- och utreseförordningen[4] definieras identitetsuppgifter primärt som uppgifter om namn, födelsedatum, medborgarskap och kön, men även biometriska uppgifter omfattas. I den reviderade Eurodacförordningen[5] definieras begreppet identitetsuppgifter i artikel 2.1.x och avser då namn, födelsedatum, medborgarskap, födelseort och kön. Att ytterligare uppgifter omfattas i nämnda förordningar – utöver vad som gäller i svensk praxis – har samband med deras respektive tillämpningsområde och syfte. Vi kan dock

[1] *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 35.
[2] *Ett säkert statligt ID-kort – med e-legitimation*, SOU 2019:14, s. 90.
[3] SOU 2021:57, s. 406.
[4] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.
[5] Europaparlamentets och rådets förordning (EU) 2024/1358 av den 14 maj 2024.

konstatera att uppgifter om namn, födelsetid och medborgarskap används i båda förordningarna. De centrala delarna i identitetsbegreppet är därmed samma som de som har växt fram i praxis på utlänningsrättens område i Sverige. Att även biometriska och andra uppgifter kan behöva kopplas till en identitet i olika register, i syfte att möjliggöra en tillförlitlig verifiering av identiteten eller identifiering av en unik individ, förändrar därför inte hur vi kommer att använda begreppet identitet i detta betänkande, det vill säga omfattande namn, födelsetid och medborgarskap.

3.3 Grundidentitet

Vår definition

Med begreppet *grundidentitet* avses i detta betänkande den identitet som bestäms och registreras av Polismyndigheten, Migrationsverket eller Skatteverket för en person.

Begreppet grundidentitet förekommer inte i författningar, förarbeten eller praxis. I Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* används begreppet i betydelsen att myndigheter fastställer uppgifter om en persons identitet när sådana uppgifter saknas i myndighetens egna register.[6] Med utgångspunkt i den definition av begreppet identitet som vi redogjort för ovan är det alltså i första hand fråga om att fastställa personens namn, födelsetid och medborgarskap. Andra uppgifter som är relaterade till identiteten kan samtidigt registreras, exempelvis om kön eller familjerelationer. En grundidentitet behöver normalt etableras när en person, av olika skäl, för första gången kommer i kontakt med svenska myndigheter. Det kan tänkas ske vid en ansökan om uppehållstillstånd eller visering men även vid folkbokföring i samband med födelse eller inflyttning till landet. En person som tidigare är okänd för svenska myndigheter kan också behöva registreras vid en gränskontroll eller inre utlänningskontroll. Utifrån de ärendeslag som är aktuella är Polismyndigheten, Migrationsverket eller Skatteverket ansvariga för att bestämma och registrera en grundidentitet.

[6] RiR 2024:12, s. 18.

Med hänsyn till att identitetsbegreppets utformning – enligt vår definition i avsnitt 3.2 – kan innebära att flera individer med samma identitet kan förekomma, och beroende på möjligheten att i ett visst ärende använda biometriska uppgifter för att identifiera en person, är det inte alltid möjligt att säkerställa att en viss individ inte redan förekommer i ett eget, eller någon annan myndighets, register. Detta kan medföra att en viss individ förekommer med multipla identiteter i svenska myndigheters register, ett problem som vi återkommer till i kapitel 9. Varje sådan identitet kan då – även om en eller flera är felaktiga – i sig anses utgöra en grundidentitet.

För vårt fortsatta arbete har den närmare definitionen av vad som utgör en grundidentitet inte någon avgörande rättslig betydelse, utan tjänar endast som ett sätt att beskriva den identitet som etableras av Polismyndigheten, Migrationsverket eller Skatteverket i något av de ärendeslag som vi redogör för i kapitel 6 och som ligger till grund för en individs fortsatta kontakter med svenska myndigheter. En sådan grundidentitet bestäms normalt först när utredningsåtgärderna avseende identiteten manifesteras på något mer konkret sätt, i första hand genom att myndigheten fattar ett beslut som medför någon form av rättsverkningar. Det kan exempelvis vara ett beslut om att avslå eller bevilja en ansökan om uppehållstillstånd eller samordningsnummer, eller ett beslut av Polismyndigheten att avvisa en utlänning i samband med en inre utlänningskontroll. Innan ett beslut fattas kan identitetsuppgifter naturligtvis behöva registreras i ärendet, men det är först när de mer slutligt bestäms, genom ett beslut av något slag, som en grundidentitet kan sägas ha etablerats. Denna behöver då i sig registreras i myndighetens system, och kommer sedan att ligga till grund för kontakter med svenska myndigheter och andra aktörer i samhället.

4 Biometri samt biometriska underlag, uppgifter och mallar

4.1 Inledning

Av våra direktiv framgår att vi bland annat ska överväga hur kopplingen till en etablerad grundidentitet kan stärkas vid verifiering av identitet, genom användning av biometriska uppgifter. Vad som avses med begreppet biometriska uppgifter får därför anses vara av central betydelse för vårt arbete. Det är även viktigt att inte blanda samman biometriska uppgifter och biometriska underlag. Vad begreppen innebär och hur vi definierar dem behöver därför inledningsvis kort behandlas.

4.2 Biometri

Det saknas en legaldefinition av begreppet biometri. Begreppet förekommer i olika sammanhang, men har inte en helt entydig innebörd. I förarbetena till brottsdatalagen (2018:1177) anges att biometri är ett samlingsnamn för automatiserad teknik med syfte att antingen identifiera en person eller avgöra om en påstådd identitet är korrekt, baserad på mätning av fysiska karaktärsdrag hos den som ska identifieras.[1] Det kan handla om att göra datorstödda jämförelser av till exempel fingeravtryck, ansiktsbilder eller röstprov. Begreppet biometri syftar alltså på den automatiserade metod eller teknik som används för att jämföra individuella kännetecken i identifierings- eller verifieringssyfte. När vi i detta betänkande använder oss av begreppet *biometri* avser vi begreppet med denna innebörd, det vill

[1] *Brottsdatalag*, prop. 2017/18:232, s. 86.

säga den teknik och metod som används för automatiserade jämförelser av olika slags individuella, biometriska, kännetecken.

4.3 Biometriska underlag

Vår definition

Med *biometriska underlag* avses i detta betänkande en persons fysiska kännetecken, bland annat ansiktsbilder och fingeravtryck.

Begreppet *biometriska underlag* används sällan i författning. Begreppet förekommer emellertid i förarbetena till brottsdatalagen och senare ändringar i lagen, där det anges att biometriska uppgifter är den information som kan tas fram ur biometriskt underlag.[2] Även i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* förekommer begreppet.[3] I 1 § förordningen (2025:145) om upptagning av biometriska underlag i brottsbekämpningen anges att förordningen innehåller bestämmelser om upptagning av prov för dna-analys, fingeravtryck, fotografi, video, röstprov, handstilsprov samt avtryck av fot och öra (biometriska underlag) enligt vissa författningar. I detta betänkande kommer vi, av läsbarhetsskäl, att ange att biometriska underlag ”tas upp” och att biometriska uppgifter ”tas fram” ur dessa.

Exempel på biometriska underlag är ansiktsbilder och fingeravtryck, men även andra individuella kännetecken så som ögats utseende, röst, händer och gångstil utgör biometriska underlag. Utifrån det biometriska underlaget går det att på teknisk väg få fram mätdata, vilket utgör biometriska uppgifter, om bearbetningen görs i syfte att åstadkomma en unik identifiering av en person eller för att avgöra om en påstådd identitet är riktig.[4] Fotografier som exempelvis bearbetas tekniskt endast för att förbättra bildkvaliteten faller alltså utanför definitionen.[5]

Även om begreppet biometriska underlag sällan används uttryckligen i författning pekas sådana underlag ut indirekt på olika sätt. Till exempel anges i 9 kap. 8 § utlänningslagen (2005:716) att det fotografi och de fingeravtryck som har tagits med stöd av första stycket 4

[2] Prop. 2017/18:232 s. 86 och *Biometri i brottsbekämpningen*, prop. 2024/25:37, s. 48.
[3] SOU 2025:75, s. 355.
[4] *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning*, Ds 2019:5 s. 143.
[5] Jfr skäl 51 till dataskyddsförordningen och prop. 2017/18:232, s. 85 f. och 435.

eller artikel 23.1 i Eurodacförordningen omedelbart ska förstöras om det framkommer att utlänningen har rätt att vistas i Sverige; fingeravtrycken och ansiktsbilden utgör de biometriska underlagen.

Som nämnts ovan kan biometriska underlag omfatta många olika fysiska kännetecken. De som i första hand används för verifiering av identitet och identifiering, exempelvis vid en gränskontroll eller en inre utlänningskontroll, och som lagras i bland annat passhandlingar, är fingeravtryck och ansiktsbilder. Dessa typer av underlag är väl beprövade och det finns utrustning och en process för hanteringen av sådana underlag hos vissa centrala myndigheter. Vi kommer därför att avgränsa våra överväganden till dessa biometriska underlag.

4.4 Biometriska uppgifter

Vår definition

Med *biometriska uppgifter* avses i detta betänkande personuppgifter som genom en särskild teknisk behandling har tagits fram ur biometriska underlag i syfte att identifiera en unik person eller verifiera en persons identitet.

Definitionen av begreppet *biometriska uppgifter* har sin grund i artikel 4.14 dataskyddsförordningen.[6] I svensk rätt definieras begreppet bland annat i 1 kap. 6 § brottsdatalagen som personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av person. Definitionen bygger på artikel 3.13 i dataskyddsdirektivet[7], men innehåller inte någon exemplifiering av olika biometriska underlag; regeringen ansåg att det kunde leda till felaktiga slutsatser om vad som omfattas.[8] I passlagen (1978:302) och utlänningslagen används i stället uttrycket *biometriska data*. Någon skillnad mot begreppet biometriska uppgifter är inte avsedd.[9] I promemorian *Ett statligt identitetskort* föreslås dock ny lydelse av bland annat av 5 a § och 6 a § passlagen, innebärande

[6] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[7] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016.
[8] Prop. 2017/18:232, s. 86.
[9] Ds 2019:5, s. 143 och *Ökad säkerhet för vissa identitets- och uppehållshandlingar – anpassning av svensk rätt till en ny EU-förordning*, Ds 2020:22, s. 70.

att begreppet biometriska data inte längre används.[10] Biometriska uppgifter utgör känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen om de behandlas för att entydigt identifiera en fysisk person (se även avsnitt 4.5).

Det är mot de biometriska uppgifterna som automatiserade jämförelser kan göras. Det är dock inte alltid dessa, utan de biometriska underlagen, som sparas i olika register. Det är även de biometriska underlagen som sparas i ett sådant digitalt lagringsmedium som finns på exempelvis ett pass eller ett uppehållstillståndskort. I detta sammanhang kan nämnas att i regeringens proposition *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* föreslås nya bestämmelser i folkbokföringslagen (1991:481) som innebär att Skatteverket ska få lagra ansiktsbilder och fingeravtryck som myndigheten har tagit upp, samt biometriska uppgifter som tas fram ur dessa.[11] I promemorian *Ett statligt identitetskort* har förslag lämnats om ett pass- och identitetskortsregister som ska få innehålla bland annat ansiktsbilder från ärenden enligt passlagen och den föreslagna lagen om statligt identitetskort *och* biometriska uppgifter som har tagits fram ur sådana ansiktsbilder.[12]

Även om det endast är de biometriska underlagen som lagras i ett visst register eller lagringsmedium anser vi att det alltid är fråga om behandling av biometriska uppgifter när underlagen tekniskt bearbetas för att kunna användas för att göra en automatisk jämförelse med en annan uppsättning biometriska uppgifter, som exempelvis har tagits fram ur fingeravtryck som har tagits upp vid en inre utlänningskontroll. Som nämnts ovan ska syftet med bearbetningen – som det anges i dataskyddsförordningen – vara att *identifiera* en unik person. Att identifiera någon innebär – som vi återkommer till i avsnitt 7.3 – i första hand att genomföra en en-till-många-kontroll mot ett register. I avsnitt 16.4.1 bedömer vi emellertid att begreppet *identifiera*, i den mening som det används i artikel 4.14 i dataskyddsförordningen, även kan anses omfatta att verifiera en persons identitet, det vill säga en en-till-en-kontroll. I detta betänkande avser vi därför – om inget annat särskilt anges – med begreppet *biometriska uppgifter* personuppgifter som genom en särskild teknisk behandling har tagits fram ur biometriska underlag i syfte att antingen identifi-

[10] Ju 2026/01595, s. 19 ff.
[11] Prop. 2025/26:261, s. 101.
[12] Ju 2026/01595, s. 143.

era en unik person eller verifiera en persons identitet, det vill säga kunna fastställa om en påstådd identitet är riktig. Det avgörande är att den tekniska bearbetningen av de biometriska underlagen görs i sådant syfte. En okulär jämförelse mellan biometriskt underlag i form av en ansiktsbild och en person som myndigheten möter utgör däremot inte behandling av biometriska uppgifter.

4.5 Biometriska mallar

Vår bedömning

Med *biometrisk mall* avses i detta betänkande en alfanumerisk representation som skapats utifrån biometriska underlag. En sådan mall utgör biometriska uppgifter enligt dataskyddsförordningen.

Biometriska underlag kan användas för att skapa en referensmall, en så kallad *biometrisk mall*, som kan jämföras mot andra sådana referensmallar, i syfte att verifiera en persons identitet eller identifiera honom eller henne.[13] Svensk rätt saknar en legaldefinition av begreppet, men i exempelvis i artikel 4.12 i EU:s förordningar om interoperabilitet[14] definieras en biometrisk mall som ”en matematisk representation som erhålls genom särdragsextraktion från biometriska uppgifter och som är begränsad till de egenskaper som är nödvändiga för att utföra identifikationer och verifieringar.” I *Guidelines on facial recognition*[15] från Europarådet uttalas att en biometrisk mall är en digital återgivning av de unika kännetecken som har hämtats från ett biometriskt prov och som kan lagras i en biometrisk databas.

En biometrisk mall är alltså ett sätt att abstrahera de biometriska underlagen. I jämförelsesfasen jämförs en biometrisk mall med andra mallar som antingen har skapats tidigare eller som skapas direkt vid jämförelsen från biometriska underlag som tagits upp tidigare. Mallen kan alltså skapas dynamiskt, i realtid, utifrån lagrade biometriska underlag och de underlag som tas upp på plats i samband med att identiteten behöver verifieras, vilket innebär behandling av biomet-

[13] Ds 2019:5, s. 143 och prop. 2024/25:37, s. 50.
[14] Europaparlamentets och rådets förordningar (EU) 2019/817 och 2019/818 av den 20 maj 2019.
[15] *Guidelines on facial recognition* (inte översatt till svenska), rådgivande kommittén för konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108), Europarådet, juni 2021.

riska uppgifter eftersom det är fråga om en teknisk bearbetning som möjliggör eller bekräftar identifieringen av en person, eller verifiering av identiteten. En biometrisk mall förväntas vara unik och specifik för varje person, och är i princip permanent över tid. Detta kan dock påverkas av typen av biometriska underlag och den enskildes ålder.[16]

Enligt den lösningshypotes med ett gemensamt identitetsindex som har utforskats av samverkansinitiativet MUR (Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärdssystemen), och som vi enligt våra direktiv ska analysera, är tanken att ett system med ett identitetindex ska möjliggöra verifiering av en persons identitet – och i vissa fall identifiering av en person – med utgångspunkt i biometri utan ett utbrett utbyte av faktiska biometriska uppgifter.[17] Det som ska lagras i ett gemensamt index är, enligt MUR:s lösningshypetes, primärt referenspunkter och individuella identitetsnycklar som bygger på en numerär översättning av jämförelse av biometriska kännetecken. Genom att jämföra biometriska uppgifter som härrör från en viss individ med biometriska uppgifter som lagrats i ett identitetsindex avseende en viss individ ska det alltså vara möjligt att verifiera personens identitet, och i vissa fall identifiera en person. För att detta ska vara möjligt behöver ett sådant identitetsindex innehålla – alternativt vid behov kunna ta fram – en biometrisk mall, i form av en numerär översättning av personens biometriska kännetecken.

Vi har svårt att se att det finns en skillnad mellan vad som avses med biometriska uppgifter respektive med en biometrisk mall. Begreppet biometrisk mall kan möjligtvis mer anses beskriva det tekniska resultatet av att omvandla biometriska underlag så att de kan användas mer effektivt för automatiska jämförelser, medan biometriska uppgifter i första hand utgör en rättslig etikett. Enligt Integritetsskyddsmyndigheten utgör en biometrisk mall – som skapas utifrån en digital ansiktsbild och består av en numerisk kod som endast kan avläsas av en datorstödd modell – biometriska uppgifter i dataskyddsförordningens mening eftersom den är unik och specifik och kan möjliggöra eller bekräfta identifiering av en fysisk person.[18] Vi delar denna bedömning. Motsvarande får enligt vår

[16] Europeiska dataskyddsstyrelsen (EDPB), *Riktlinjer 05/2022 om användningen av teknik för ansiktsigenkänning på brottsbekämpningsområdet*, den 26 april 2023, s. 10.
[17] *Behov av en sammanhållen infrastruktur för identitet*, Skatteverket, dnr 8/2765903, 2024-01-19.
[18] https://www.imy.se/verksamhet/dataskydd/innovationsportalen/vagledning-om-ansiktsigenkanning-och-gdpr/gdpr-och-ansiktsigenkanningsteknik/, hämtad 2025-06-05.

bedömning anses gälla en biometrisk mall som skapas utifrån fingeravtryck.

En biometrisk mall, som skapats utifrån en persons biometriska underlag, är enligt vår bedömning alltså biometriska uppgifter enligt definitionen i artikel 4.14 i dataskyddsförordningen. Det faktum att mallen är tekniskt begränsad till de egenskaper som är nödvändiga för att identifiera någon eller verifiera identiteten medför ingen annan bedömning. En alfanumerisk representation som skapats utifrån biometriska underlag är därmed biometriska uppgifter enligt dataskyddsförordningen.

5 Allmänt om dataskydd och grundläggande rättigheter

5.1 Inledning

I vårt uppdrag ingår att analysera om biometriska uppgifter kan och bör användas i större utsträckning för att främja en säker verifiering av identitet. Behandling av personuppgifter kan innebära risker för intrång i skyddet för den personliga integriteten enligt regeringsformen, den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). Behandling av biometriska uppgifter kan medföra särskilda sådana risker. Behovet av att behandla olika typer av personuppgifter i syfte att möjliggöra säker verifiering av identitet måste därför vägas mot behovet av skydd för grundläggande fri- och rättigheter. Vidare innehåller både det EU-rättsliga och nationella dataskyddsregelverket bestämmelser om behandling av personuppgifter som behöver beaktas vid våra fortsatta överväganden.

Det finns anledning att redan här översiktligt redogöra för de relevanta rättsliga ramarna i dessa avseenden. Någon fullständig redogörelse för de aktuella regelverken är enligt vår bedömning inte nödvändig utan vi har begränsat detta kapitel till de delar som kan få direkt betydelse för våra överväganden, utifrån det uppdrag vi har. Vi återkommer med de bedömningar som behöver göras i fråga om dataskydd och skydd för den personliga integriteten i samband med att dessa frågor gör sig gällande i olika delar av betänkandet (se framför allt kapitel 16, 17, 21 och 24).

5.2 Dataskydd

Dataskydd är ett begrepp som används för att ange skyddet för den personliga integriteten i de regelverk som ska tillämpas vid behandling av personuppgifter. Dataskyddsreglerna har alltså sin grund i de mänskliga rättigheterna och då främst i rätten till skydd för den personliga integriteten, som bland annat kommer till uttryck i artikel 8 i Europakonventionen och artikel 3 i EU:s rättighetsstadga. Bestämmelser som reglerar personuppgiftsbehandling finns i dataskyddsförordningen[1], som ofta kallas för sin engelska förkortning, GDPR. Vi använder emellertid det svenska namnet dataskyddsförordningen. Förordningen innehåller bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag. I Sverige kompletteras dataskyddsförordningen av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) samt tillhörande förordning (2018:219). I detta avsnitt redogör vi för relevanta delar av dessa författningar.

5.2.1 Dataskyddsförordningen

Dataskyddsförordningen är till alla delar bindande och direkt tillämplig i EU:s medlemsstater. Den ska alltså tillämpas av enskilda och myndigheter som om det vore nationella författningsbestämmelser. Från tillämpningsområdet undantas personuppgiftsbehandling som utförs av behöriga myndigheter – i Sverige exempelvis Polismyndigheten – i syfte att förebygga, förhindra, eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder samt upprätthålla allmän ordning och säkerhet. Personuppgiftsbehandling som utförs för dessa syften, av behöriga myndigheter, omfattas i stället av dataskyddsdirektivets[2] och brottsdatalagens (2018:1177) tillämpningsområde.

Dataskyddsförordningen syftar bland annat till att skydda enskildas grundläggande rättigheter och friheter, särskilt deras skydd av personuppgifter. Förordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis sker på automatisk väg och på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. I förordningen regleras bland

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[2] Europaparlamentets och rådets förordning (EU) 2016/680 av den 27 april 2016.

annat grundläggande principer för behandling av personuppgifter, den registrerades rättigheter, personuppgiftsansvar, överföring av personuppgifter, tillsyn över personuppgiftsbehandling, rätten för enskilda att få tillgång till rättsmedel, och sanktioner mot ansvariga som inte lever upp till förordningens krav.

Begreppet *personuppgifter* definieras i artikel 4.1 i förordningen. Det har en vidsträckt innebörd och omfattar alla upplysningar som avser en identifierad eller identifierbar person; ”en registrerad”. Begreppet omfattar däremot inte uppgifter om avlidna fysiska personer (se skäl 27). Även definitionen av begreppet *behandling* är vid och omfattar i princip alla åtgärder som vidtas i fråga om personuppgifter. Den uppräkning som görs i artikel 4.2 är inte uttömmande och anger bland annat insamling, registrering, lagring, användning och spridning som exempel på behandling. Alla åtgärder eller kombinationer av åtgärder beträffande uppgifter som avser en identifierad eller identifierbar person utgör alltså behandling av personuppgifter.

5.2.2 Dataskyddslagen

Dataskyddslagen innehåller nationella bestämmelser som kompletterar dataskyddsförordningen och förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen. Dataskyddslagen är enligt 1 kap. 6 § subsidiär i förhållande till annan lag eller förordning, vilket innebär att avvikande bestämmelser för specifika verksamheter eller myndigheter har företräde. Sådana avvikande bestämmelser finns i en rad registerförfattningar, som reglerar behandlingen av personuppgifter i en viss verksamhet eller hos en viss myndighet. Som exempel kan nämnas domstolsdatalagen (2015:728) och utlänningsdatalagen (2016:27). Syftet med registerförfattningar är att anpassa lagstiftningen till de behov som finns inom olika verksamhetsområden och samtidigt göra avvägningar mot behovet av skydd för enskildas integritet.

Dataskyddslagen och dataskyddsförordningen ska, enligt 1 kap. 7 §, inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

5.2.3 Grundläggande principer för personuppgiftsbehandling

De grundläggande krav som måste följas vid all personuppgiftsbehandling framgår av artikel 5.1 i dataskyddsförordningen. Av bestämmelsen framgår att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska inte anses vara oförenliga med de ursprungliga ändamålen (ändamålsbegränsning eller finalitetsprincipen). Uppgifterna ska vidare vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen (uppgiftsminimering) samt riktiga och, om det är nödvändigt, uppdaterade. Alla rimliga åtgärder ska vidtas för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål (riktighet). Personuppgifter får inte förvaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (lagringsminimering) och de ska skyddas genom lämpliga säkerhetsåtgärder (integritet och konfidentialitet).

Enligt artikel 5.2 i dataskyddsförordningen är det den personuppgiftsansvarige som ska säkerställa att kraven följs vid behandlingen av uppgifterna.

Rättslig grund för att behandla personuppgifter

För att en behandling av personuppgifter ska vara laglig måste den vila på en rättslig grund enligt artikel 6.1 i dataskyddsförordningen. De rättsliga grunderna är samtycke, avtal, rättslig förpliktelse, grundläggande intresse, allmänt intresse, myndighetsutövning och intresseavvägning. Uppräkningen i artikel 6.1 är uttömmande. Grunderna är i viss mån överlappande och flera rättsliga grunder kan vara tillämpliga avseende en och samma behandling.[3] De rättsliga grunder som enligt vår bedömning framför allt kan bli aktuella i förhållande till den behandling av personuppgifter som kan förekomma vid verifiering av identitet är samtycke, allmänt intresse, myndighetsutövning och avtal.

[3] *Ny dataskyddslag*, prop. 2017/18:105, s. 46.

- *Samtycke* av den registrerade definieras i artikel 4.11 i dataskyddsförordningen som varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne. Om den registrerade har lämnat sitt samtycke till en behandling av personuppgifter krävs det inte att behandlingen är nödvändig, vilket är fallet vid tillämpning av övriga rättsliga grunder. Det unionsrättsliga begreppet har dock inte samma strikta innebörd som det svenska ordet nödvändig och det bör i dagsläget mer eller mindre regelmässigt anses vara nödvändigt att använda tekniska hjälpmedel och därmed behandla personuppgifter på automatisk väg, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för vare sig myndigheter eller privata aktörer.[4]
- Enligt artikel 6.1 e i dataskyddsförordningen får personuppgifter behandlas om behandlingen är nödvändig för att utföra en uppgift av *allmänt intresse*. Alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är enligt regeringens mening av allmänt intresse. På motsvarande sätt är de obligatoriska uppgifter som ålagts kommuner och landsting att utföra av allmänt intresse. Om uppgifterna inte vore av allmänt intresse skulle myndigheterna inte ålagts att utföra dem. Detta får anses gälla även i dataskyddsförordningens mening, eftersom det är upp till varje medlemsstat att fastställa de uppgifter som är av allmänt intresse. Även en privat aktör som fullgör ett uppdrag från en myndighet avseende en sådan uppgift som är fastställd i författning, regeringsbeslut eller kommunalt beslut i fullmäktige kan vidta nödvändiga personuppgiftsbehandlingsåtgärder på samma rättsliga grund som om myndigheten själv utfört uppgiften.[5]
- Om behandlingen är nödvändig som ett led i den personuppgiftsansvariges *myndighetsutövning* är den tillåten, enligt artikel 6.1 e i dataskyddsförordningen. Myndighetsutövning innebär en befogenhet att i förhållande till en enskild bestämma om förmån, rättighet, skyldighet, disciplinär bestraffning eller annat jämförbart förhållande. Befogenheten kan grunda sig på ett konkret beslut av regeringen eller riksdagen men grundas vanligtvis på bestäm-

[4] Prop. 2017/18:105, s. 46 f.
[5] Prop. 2017/18:105, s. 56 ff.

melser i den offentligrättsliga lagstiftningen som ger en myndighet en rätt eller skyldighet att agera på ett visst sätt. I propositionen *Bättre möjligheter att samverka vid medborgarkontor* uttalades bland annat att till myndighetsutövning kan hänföras inte bara beslut som innehåller direkta handlingsmönster i förhållande till den enskilde utan även beslut som har indirekta rättsverkningar, till exempel registreringsbeslut. Karakteristiskt för myndighetsutövning är att den enskilde befinner sig i någon form av beroendeförhållande till myndigheten.[6] Den rättsliga grunden myndighetsutövning kan tillämpas av alla personuppgiftsansvariga som tilldelats myndighetsutövande befogenheter.[7]

- Behandling av personuppgifter kan enligt artikel 6.1 b ske för att *fullgöra ett avtal* i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Detta stöder indirekt näringsfriheten och speglar det faktum att de avtalsenliga skyldigheterna gentemot den registrerade ibland inte kan uppfyllas utan att vissa personuppgifter om honom eller henne kan behandlas. Om den särskilda behandlingen utgör en integrerad del i tillhandahållandet av den begärda tjänsten ligger behandlingen av dessa uppgifter i båda parters intresse, eftersom tjänsten i annat fall inte kan tillhandahållas och avtalet inte kan fullgöras.

Behandling som utförs med stöd av någon av de rättsliga grunderna allmänt intresse eller myndighetsutövning måste vara fastställd i unionsrätten eller i nationell rätt i enlighet med artikel 6.3. Detta innebär dock inte ett krav på att själva behandlingen av personuppgifter måste regleras. Det är i stället den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen.[8] De rättsliga grunderna uppgift av allmänt intresse och myndighetsutövning regleras i 2 kap. 2 § dataskyddslagen.

[6] Prop. 1996/97:90, s. 26.
[7] Prop. 2017/18:105, s. 62 f.
[8] Prop. 2017/18:105, s. 48.

5.2.4 Särskilt om känsliga personuppgifter

För behandling av särskilda kategorier av personuppgifter – i svensk rätt kallade känsliga personuppgifter – finns särskilda bestämmelser i dataskyddsförordningen. Det gäller bland annat behandling av biometriska uppgifter. Behandling av känsliga personuppgifter är enligt huvudregeln i artikel 9.1 i dataskyddsförordningen förbjuden.

Undantag för att behandla känsliga personuppgifter

Det finns ett flertal undantag från förbudet i artikel 9.1 i dataskyddsförordningen. Dessa framgår av artikel 9.2. Undantagen kan sägas innehålla rättsliga grunder för att få behandla känsliga personuppgifter. Bestämmelsen innehåller en uttömmande uppräkning av de situationer då behandling av känsliga personuppgifter kan få förekomma. Undantagen ska tolkas restriktivt.[9] Bland möjliga undantag finns samtycke och att behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, vilket framgår av artikel 9.2 a och g. Det kan noteras att artikel 9.2 inte erkänner grunden *nödvändig för att fullgöra ett avtal* (jfr artikel 6.1 c) som ett undantag från förbudet att behandla känsliga personuppgifter. För privata aktörer kan det enda möjliga lagliga undantaget för att behandla känsliga personuppgifter ofta vara att få ett uttryckligt samtycke från den registrerade.[10]

Medlemsstaterna får enligt artikel 9.4 i dataskyddsförordningen behålla eller införa ytterligare villkor, även begränsningar, för behandling av biometriska uppgifter. Sådana bestämmelser finns bland annat i registerförfattningar – exempelvis i 14 § utlänningsdatalagen – men även i 3 kap. dataskyddslagen. Bestämmelsen i 3 kap. 3 § dataskyddslagen reglerar närmare när känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 i dataskyddsförordningen. Bestämmelsen är enligt förarbetena avsedd att gälla för offentlig verksamhet där sektorspecifik reglering avseende behandling av känsliga personuppgifter saknas. Vidare anfördes i förarbetena att det kan finnas anledning för vissa sektorer att närmare precisera och avgränsa möjligheterna att behandla känsliga personuppgifter, men även att det kan finnas ett berättigat behov av att behandla

[9] Se till exempel EU-domstolens dom i mål C-252/21, *Meta Platforms Inc*, punkt 76.
[10] Jfr Artikel 29-gruppens riktlinjer om samtycke enligt förordning 2016/679 (WP259), som stöds av europeiska dataskyddsstyrelsen (EDPB), s. 19.

känsliga personuppgifter i en större omfattning än vad dessa bestämmelser medger.[11] I fråga om brottsbekämpande verksamhet finns särskilda bestämmelser i 2 kap. 11 och 12 §§ brottsdatalagen.

5.2.5 Särskilt om person- och samordningsnummer

Person- och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men har ändå en särställning genom att medlemsstaterna har möjlighet att införa särskilda villkor för behandlingen av sådana uppgifter. Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt förordningen (artikel 87).

Enligt dataskyddslagen får personnummer och samordningsnummer behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl (3 kap. 10 §). Den som ska behandla person- eller samordningsnummer ska alltså göra en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som behandlingen innebär. Vid intresseavvägningen bör omständigheter som exempelvis om det eftersträvade syftet med behandlingen kan uppnås på annat sätt, behandlingens omfattning och om behandlingen förutsätter samkörning av register tillmätas betydelse.[12] Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten (3 kap. 11 §). Någon generell föreskrift har inte meddelats av regeringen i förordning (2018:219), men det är relativt vanligt med sektorspecifika bestämmelser.

[11] Prop. 2017/18:105, s. 91.
[12] Prop. 2017/18:105, s. 199.

5.2.6 Dataskyddsdirektivet och brottsdatalagen

Dataskyddsförordningen är inte tillämplig på den behandling av personuppgifter som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder (artikel 2.2 d). För personuppgiftsbehandling inom detta område gäller i stället dataskyddsdirektivet, som har genomförts i Sverige i huvudsak genom brottsdatalagen. Det är alltså myndighetens syfte med behandlingen av personuppgifter som är avgörande för vilket regelverk som blir tillämpligt. Med behörig myndighet avses primärt en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte (1 kap. 6 § brottsdatalagen). Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, Ekobrottsmyndigheten, Åklagarmyndigheten, de allmänna domstolarna och Kriminalvården är behöriga myndigheter, men enbart när de behandlar personuppgifter för sådana syften.[13]

Brottsdatalagen är – liksom dataskyddslagen – subsidiär (1 kap. 5 §) och kompletteras av nationell rätt som innehåller preciseringar, undantag och avvikelser från brottsdatalagen. För Polismyndigheten gäller lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, med tillhörande förordning (2018:1942). För Skatteverket gäller lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område, med tillhörande förordning (2018:1877).

I 2 kap. brottsdatalagen finns bestämmelser om grundläggande krav på personuppgiftsbehandling, bland annat bestämmelser om rättslig grund för behandlingen. Lagen innehåller också särskilda bestämmelser om behandling av känsliga personuppgifter. Biometriska uppgifter får endast behandlas om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen (12 §). Kravet på att det ska vara absolut nödvändigt innebär att behovet av att behandla sådana uppgifter måste prövas särskilt noga.

[13] Se Sandén, *Brottsdatalagen*, JUNO version 1 E, 2024-06-05, kommentaren till 1 kap. 2 §.

5.3 Skydd för den personliga integriteten

Som nämnts inledningsvis i detta kapitel kan behandling av personuppgifter innebära risker för intrång i skyddet för den personliga integriteten. Regeringsformen, Europakonventionen och EU:s rättighetsstadga innehåller bestämmelser om skydd för sådana rättigheter. Under vissa förutsättningar får rättigheterna emellertid inskränkas. Den slutliga bedömningen av om en viss nationell rättsregel som inskränker en grundläggande rättighet är proportionerlig ankommer i första hand på EU-domstolen och Europadomstolen. I detta avsnitt redogör vi översiktligt för skyddet för den personliga integriteten och förutsättningarna för inskränkning av skyddet.

5.3.1 Regeringsformen

Av 2 kap. 6 § första stycket regeringsformen framgår att var och en är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp. Uttrycket *kroppsligt ingrepp* avser i första hand våld mot människokroppen, men även smärre ingrepp som vaccinering och liknande företeelser.[14] Att ta fingeravtryck omfattas av skyddet mot påtvingade kroppsliga ingrepp, medan det inte utgör ett kroppsligt ingrepp i den mening som avses i bestämmelsen att fotografera någon.[15]

Vidare är var och en, enligt 2 kap. 6 § andra stycket regeringsformen, skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Med *enskilds personliga förhållanden* avses samma som i tryckfrihetsförordningen och offentlighets- och sekretesslagstiftningen, vilket innebär att regleringen träffar till exempel uppgifter om namn och andra identifikationsuppgifter, adress, familjeförhållanden och fotografier.[16] Exempel på uppgiftssamlingar som innebär kartläggning är misstanke-, fingeravtrycks- och DNA-register.

Vad som är ett betydande intrång får bedömas utifrån åtgärdens intensitet och omfattning samt uppgifternas integritetskänsliga natur. Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning av den enskildes personliga förhållanden är inte

[14] Prop. 1975/76:209 *om ändring i regeringsformen*, s. 147.
[15] *Kontroll av biometriska kännetecken i resehandlingar*, prop. 2017/18:35 s. 12.
[16] *Biometri i brottsbekämpningen,* prop. 2024/25:37, s. 47.

åtgärdens huvudsakliga syfte, utan vilken effekt den har. Vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden är det naturligt att stor vikt läggs vid uppgifternas karaktär. Ju känsligare uppgifterna är, desto mer ingripande måste det allmännas hantering av uppgifterna normalt anses vara. Även hantering av ett fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. Även mängden uppgifter kan vara en betydelsefull faktor i sammanhanget.[17]

Skyddet mot intrång som innebär övervakning och kartläggning av den enskildes personliga förhållanden och skyddet mot annat kroppsligt ingrepp än döds- och kroppsstraff får enligt 2 kap. 20 § regeringsformen begränsas genom lag, i den utsträckning som medges i 21–24 §§. Av 21 § följer att begränsningar får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och att begränsningen aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Vidare får begränsningen inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

För andra än svenska medborgare får särskilda begränsningar i lag göras bland annat av skyddet mot integritetsintrång och kroppsligt ingrepp (2 kap. 25 § regeringsformen). De förutsättningar för begränsningar av fri- och rättigheter som anges i 21, 22 och 24 §§ gäller inte för begränsningar som tar sikte enbart på utlänningar. Dock innehåller även Europakonventionen regler om hur inskränkningar av fri- och rättigheter får göras (se avsnitt 5.3.2) och lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen (2 kap. 19 § regeringsformen). Av praktiska skäl är det endast undantagsvis som det går att göra skillnad på svenska medborgare och utlänningar i lagstiftningen. I befintlig lagstiftning är det väsentligen i utlänningslagstiftningen som sådan särbehandling förekommer. Utlänningslagen (2005:716) innehåller till exempel flera inskränkningar av de grundlagsskyddade fri- och rättigheterna som avser utländska medborgare.

[17] *En reformerad grundlag*, prop. 2009/10:80, s. 180 ff.

5.3.2 Europakonventionen

Europakonventionen gäller som lag i Sverige. Enligt artikel 8.1 har var och en rätt till respekt för bland annat sitt privat- och familjeliv. Skyddet enligt artikel 8 spänner över en rad områden. Privatliv är en bred term som inte går att uttömmande definiera. Det omfattar dock både fysisk och personlig integritet. Europadomstolen har i flera fall konstaterat att artikel 8 ålägger medlemsstaterna 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 exempelvis *Airey mot Irland,* nr 6289/73, *X och Y mot Nederländerna*, nr 8978/80 och *Söderman mot Sverige*, nr 5786/08). Att ta någons fingeravtryck utgör ett intrång i privatlivet (se s. *och Marper mot Storbritannien*, nr 30562/04 och 30566/04). Detsamma gäller att ta fotografier av en person utan dennes samtycke (se bland annat *von Hannover mot Tyskland*, nr 59320/00).

Redan att en myndighet behandlar eller registrerar uppgifter om en persons privatliv, det vill säga personuppgifter, kan i vissa fall utgöra en inskränkning av rätten till skydd för privatlivet (se Europadomstolens avgörande i *Leander mot Sverige*, nr 9248/81). I det ovan nämnda målet s. *och Marper mot Storbritannien* uttalade Europadomstolen att skyddet av personuppgifter är av grundläggande betydelse för en persons åtnjutande av sin rätt till respekt för privat- och familjeliv, att den nationella lagstiftningen måste ge lämpliga skyddsåtgärder för att förhindra sådan användning av personuppgifter som kan vara oförenlig med garantierna i artikel 8, och att behovet av sådana skyddsåtgärder är desto större när det gäller skyddet av personuppgifter som genomgår automatisk behandling, inte minst när sådana uppgifter används för polisändamål. Enligt domstolen bör det särskilt säkerställas att sådana uppgifter är relevanta och inte alltför omfattande i förhållande till de ändamål för vilka de lagras, och att de inte bevaras i en form som möjliggör identifiering av de registrerade längre än vad som krävs för det ändamål för vilket dessa uppgifter lagras (punkt 103). Målet *Glukhin mot Ryssland,* nr 11519/20, rörde ryska myndigheters användning av ansiktsigenkänningsteknik i samband med demonstrationer. Domstolen slog fast att behandlingen av den enskildes personuppgifter under demonstrationen var påträngande och oförenlig med värderingarna i ett demokratiskt samhälle.

Användningen av ansiktsigenkänningsteknik ansågs onödig och oproportionerlig. Dessutom noterade domstolen att det saknades detaljerade regler och skyddsåtgärder som skulle reglera användningen av sådan teknik i nationell lag.

Artikel 8.2 ger möjlighet att inskränka skyddet för privat- och familjeliv med stöd av lag om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter. Av Europadomstolens praxis framgår att laglighetskriteriet bland annat innebär att den nationella författningen måste uppfylla vissa minimikrav i fråga om kvalitet och tydlighet. Reglerna ska vara tillräckligt tydliga för att tillämpningen ska vara förutsebar, och de ska vara allmänt tillgängliga. Kravet att ett ingripande ska vara nödvändigt i ett demokratiskt samhälle innebär att det ska finnas ett angeläget samhälleligt behov av åtgärden i fråga. I det ligger bland annat en begränsning som innebär att åtgärden inte får gå längre än vad som är nödvändigt med beaktande av proportionalitetsprincipen, det vill säga begränsningen ska stå i rimlig relation till det intresse som åtgärden är avsedd att tillgodose (se ovan nämnda mål s. *och Marper mot Storbritannien* och *Glukhin mot Ryssland*). Varje konventionsstat har själv en viss frihet att avgöra om en inskränkning är nödvändig; Europadomstolen förbehåller sig rätten att övervaka om så är fallet.[18]

5.3.3 EU:s rättighetsstadga

Den personliga integriteten skyddas också av EU:s rättighetsstadga, som innehåller både preciserade rättigheter och allmänna principer. I artikel 3, 7 och 8 slås bland annat fast att var och en har rätt till integritet, respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter. Enligt stadgan måste varje begränsning i utövandet av de fri- och rättigheter som erkänns i stadgan vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot

[18] Se Danelius, Danelius, Bull och Cameron, *Mänskliga rättigheter i europeisk praxis*, 2023, version 6, JUNO, s. 443.

mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter (artikel 52.1).

Av EU-domstolens praxis avseende begränsning av de rättigheter som följer av artikel 7 och 8 framgår följande generella utgångspunkter. Undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är absolut nödvändigt (se bland annat de förenade målen C-203/15 och C-698/15, *Tele2 Sverige AB och Secretary of State for the Home Department mot Post- och telestyrelsen m.fl.* och mål C-140/20, *G.D. mot Commissioner of the Garda Síochána m.fl.*).

När det finns flera ändamålsenliga åtgärder att välja mellan för att uppnå det legitima mål som eftersträvas, ska den åtgärd väljas som är minst ingripande. En balanserad avvägning ska göras mellan å ena sidan målet av allmänt samhällsintresse och å andra sidan de berörda rättigheterna, för att säkerställa att de olägenheter som åtgärderna medför inte är orimliga i förhållande till de eftersträvade målen. Möjligheten att motivera en begränsning av rättigheter ska bedömas utifrån allvaret i det ingrepp som rättighetsbegränsningen medför och genom en prövning av huruvida betydelsen av det mål av allmänt intresse som eftersträvas med denna begräsning står i proportion till ingreppets allvar (se EU-domstolens dom i mål C-61/22, *Landeshaupstadt Wiesbaden*, punkt 83). En prövning mot proportionalitetsprincipen innefattar, enligt EU-domstolen, en prövning i tre led. Prövningen avser i det första ledet om åtgärden i fråga eftersträvar ett eller flera av unionen erkända mål av allmänt samhällsintresse och faktiskt är ägnad att uppnå dessa mål. I det andra ledet är fråga om rättighetsingreppen är begränsade till vad som är absolut nödvändigt, i den meningen att målen inte rimligen skulle kunna uppnås lika effektivt med andra medel som innebär ett mindre intrång i de berörda personernas grundläggande rättigheter. I det tredje ledet prövas om ingreppen står i rimlig proportion till de eftersträvade målen, vilket bland annat innefattar en avvägning mellan dessa mål och ingreppets allvar (se punkt 84).

6 Ärenden där en identitet kan behöva etableras

6.1 Inledning

Polismyndigheten, Migrationsverket och Skatteverket har en central roll i den statliga identitetsförvaltningen genom att de ansvarar för att i vissa ärendeslag verifiera identitet för personer som vistas, eller vill vistas, i Sverige och – för det fall det inte kommer fram att personen är känd för svenska myndigheter sedan tidigare – bestämma och registrera en grundidentitet. I vissa av de ärendeslag då nämnda myndigheter möter en person ligger fokus på att bestämma en grundidentitet, framför allt i ärenden om folkbokföring vid födsel i eller inflyttning till Sverige, vid tilldelning av samordningsnummer och vid ansökan om visering eller uppehållstillstånd innan eller i samband med inresa till Sverige. Även vid gränskontroller och inre utlänningskontroller kan en grundidentitet behöva bestämmas i vissa fall.

Gemensamt för samtliga ovan nämnda ärenden är att utredningen av identiteten är av central betydelse. Detsamma kan visserligen sägas för ett ärende om medborgarskap genom naturalisation och om utfärdande av hemlandspass, identitetskort och uppehållstillståndskort. I dessa fall kommer däremot normalt inte någon grundidentitet att behöva etableras utan identiteten behöver i stället verifieras och, i undantagsfall, uppdateras; till exempel kan nya uppgifter om identiteten komma fram vid ansökan om naturalisation, genom att sökanden lämnar in ett hemlandspass som inte fanns tillgängligt när en grundidentitet etablerades i ett tidigare ärende om internationellt skydd. Det är enligt vår uppfattning dock inte fråga om att bestämma en grundidentitet i en sådan situation. Den identitet som då kan sägas etableras kommer däremot att ligga till grund för personens framtida kontakter med aktörer i det svenska samhället, vid vilka identiteten

kan behöva verifieras. En annan gemensam nämnare för de ärenden där en grundidentitet ofta behöver bestämmas är att det finns ett gällande, beslutat eller föreslaget rättsligt stöd för att använda biometriska uppgifter under processen för att kontrollera och verifiera identitet eller identifiera en person. I kapitel 7 redogör vi närmare för detta. Som utgångspunkt för den redogörelsen kan en kort redovisning av de olika ärendeslag där en grundidentitet kan behöva etableras vara av värde.

6.2 Migrationsverket och utlandsmyndigheterna

Migrationsverket ansvarar för att verifiera identitet när en utlänning ansöker om uppehållstillstånd eller svenskt medborgarskap. Migrationsverket får i enlighet med 3 kap. 5 § utlänningslagen (2005:716) även handlägga en ansökan om visering, men det är i normalfallet utlandsmyndigheterna som både genomför utredningsåtgärder och fattar beslut i ärenden om visering.

6.2.1 Uppehållstillstånd

Grunden för svensk utlänningslagstiftning är principen om en reglerad invandring. Det innebär bland annat att det för tredjelandsmedborgare som huvudregel krävs uppehållstillstånd för att få vistas i Sverige och att ett sådant tillstånd ska ha beviljats före inresan i landet. Uppehållstillstånd kan beviljas exempelvis på grund av skyddsskäl, anknytning till någon som bor i Sverige, arbete eller synnerligen ömmande omständigheter.

Det är Migrationsverket som beslutar i ärenden om uppehållstillstånd och myndigheten behöver då vidta olika utredningsåtgärder för att verifiera utlänningens identitet eller identifiera honom eller henne. Identiteten ska som utgångspunkt vara styrkt i tillståndsärenden. Med hänsyn till att en ansökan i många fall kan avslås redan på grund av att detta beviskrav inte är uppfyllt finns det ett naturligt incitament för sökanden att medverka till att klarlägga sin identitet och lämna över de handlingar som krävs för detta. För att en sökande ska anses ha styrkt sin identitet på ett godtagbart sätt ska han eller hon som huvudregel kunna visa ett pass i original (se MIG 2009:7) eller en fotoförsedd identitetshandling i original utfärdad av behörig

myndighet i hemlandet. Den utredningsmetod som aktualiseras i ärenden om uppehållstillstånd är i första hand en granskning av dessa dokument och verifiering av identiteten kan då ske mot innehållet i handlingarna. I vissa fall gäller undantag från huvudregeln att identiteten ska vara styrkt, bevislättnad, det vill säga det är tillräckligt att sökanden gör sin identitet sannolik. Så är fallet bland annat i ärenden om internationellt skydd[1] och i vissa ärenden om familjeåterförening (se exempelvis MIG 2011:11, MIG 2014:16 och MIG 2016:13). När det gäller personer som ansökt om internationellt skydd framgår av statistik från Migrationsverket för år 2012 till 2023 att endast cirka 25 procent av de som beviljades uppehållstillstånd på sådan grund hade visat upp en giltig passhandling.[2] En möjlighet att ta upp biometriska underlag och att söka i EU-gemensamma och nationella register är då viktiga instrument för att verifiera identiteten. Bestämmelser kring sådana möjligheter finns i flera EU-förordningar, bland annat gränsförordningen[3] och in- och utreseförordningen[4]. Även muntliga intervjuer, medicinska åldersbedömningar och språkanalyser kan användas för att utreda identitet, även om dessa åtgärder får anses vara behäftade med tillförlitlighetsbrister. Nämnda utredningsåtgärder innefattar vanligtvis ett krav på att utlänningen inställer sig personligen, antingen vid en svensk ambassad utomlands eller vid någon av Migrationsverkets enheter i Sverige.

6.2.2 Schengenviseringar och nationella viseringar

En visering utfärdas för tillfälliga besök och måste ansökas om innan inresan. Syftet med en visering kan vara att besöka släkt eller vänner, ett turistbesök, ett affärsbesök eller en genomresa. Det finns två huvudtyper av visering: Schengenvisering och nationell visering. En utlänning som reser in i eller vistas i Sverige ska som utgångspunkt, enligt 2 kap. 3 § utlänningslagen, ha någon av dessa typer av visering. Kravet på visering gäller dock inte för en utlänning som är EES-medborgare eller har uppehållstillstånd (se 2 kap. 8 a § utlännings-

[1] Med anledning av införandet av EU:s migrations- och asylpakt har terminologin för asylförfarandet ändrats. Bland annat ska begreppet ”asyl” utmönstras till förmån för ”internationellt skydd”, se *Utmönstring av permanent uppehållstillstånd och anpassning av svensk rätt till EU:s migrations-och asylpakt*, prop. 2025/26:262, s. 157 ff.
[2] Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter*, RiR 2024:12, s. 34.
[3] Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018.
[4] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.

lagen) och det finns en förteckning över tredjeländer vilkas medborgare är skyldiga att inneha visering när de passerar de yttre gränserna och över de tredjeländer vars medborgare är undantagna från detta krav.

Enligt huvudregeln är utlandsmyndigheterna behöriga att handlägga en ansökan om visering. Villkoren för utfärdande av en Schengenvisering regleras uttömmande i viseringskodexen[5]. En Schengenvisering kan beviljas för planerade vistelser på medlemsstaternas territorium som inte varar längre än 90 dagar under en 180-dagarsperiod. En tredjelandsmedborgare som vill besöka Sverige i mer än 90 dagar behöver i stället antingen ansöka om uppehållstillstånd för besök eller om en nationell visering. En nationell visering får beviljas endast om det finns särskilda skäl och endast för längre tid än tre månader, dock högst ett år (3 kap. 4 § utlänningslagen). I förarbetena nämns som exempel på särskilda skäl att det rör sig om nära släktingar som önskar vistas i Sverige längre tid än tre månader eller att det kan vara fråga om affärsbesök.[6]

Den som ansöker om en Schengenvisering ska, enligt artikel 12 i viseringskodexen, ge in en giltig resehandling som uppfyller vissa kriterier avseende till exempel giltighetstid. Något uttryckligt beviskrav för nationell visering finns inte i utlänningslagen, varken vad gäller sökandens identitet eller de särskilda skäl som krävs för beviljande av visering. En klarlagd identitet är dock en förutsättning för ställningstagande till om det finns särskilda skäl för att bevilja visering, och för att en tredjelandsmedborgare ska uppfylla inresevillkoren enligt gränskodexen[7] krävs att han eller hon innehar en giltig resehandling. Vid prövningen av en ansökan om visering har myndigheterna därför att verifiera sökandens identitet genom att kontrollera dennes resehandling, vilket är det främsta sättet att styrka identiteten. Även andra metoder kan vara av betydelse i vissa situationer, som till exempel sökningar i olika register och muntliga intervjuer. För utbyte av uppgifter om viseringar mellan EU:s medlemsländer finns Visa Information System (VIS), som regleras i VIS-förordningen[8].

[5] Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009.
[6] *Ny instans- och processordning i utlännings- och medborgarskapsärenden*, prop. 2004/05:170 s. 272 f. och *EU:s viseringskodex*, prop. 2010/11:121 s. 36.
[7] Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016.
[8] Europaparlamentets och rådets förordning (EU) nr 767/2008 av den 9 juli 2008.

6.2.3 Förslag om registrering av EES-medborgare i vissa fall

Enligt nu gällande bestämmelser i utlänningslagen saknas krav på att en EES-medborgare som vistas i Sverige med uppehållsrätt under en längre tid än tre månader ska registrera vistelsen hos svenska myndigheter. Eftersom EES-medborgare som utgångspunkt inte behöver uppehållstillstånd för att vistas i landet kommer en grundidentitet för denna kategori av personer därför normalt att etableras först när de folkbokförs eller tilldelas ett samordningsnummer (se avsnitt 6.4); EES-medborgare som vistas i landet med uppehållsrätt under kortare tid än ett år ska inte bli folkbokförda och behöver därför inte heller anmäla sin inflyttning till Skatteverket. För att utöka myndigheternas tillgång till information om dessa personer har förslag lämnats i betänkandet *Registrering av EES-medborgare* om att återinföra en registreringsskyldighet för EES-medborgare vid vistelser i Sverige som överstiger tre månader.[9]

Enligt förslagen i betänkandet ska Migrationsverket ansvara för registreringsförfarandet. I samband med utfärdande av ett registreringsbevis ska myndigheten få kräva att sökanden visar upp ett giltigt pass eller ett giltigt identitetskort. Myndigheten ska också få fotografera sökanden och ta hans eller hennes fingeravtryck, i syfte att biometriskt verifiera sökandens identitet mot den handling som han eller hon har visat upp. Uppgifter om bland annat EES-medborgarens identitet kommer att få registreras i den centrala utlänningsdatabasen.[10] På detta sätt kommer, som vi ser det, i många fall en grundidentitet att etableras av Migrationsverket inom ramen för ett ärende om registrering av EES-medborgaren, i ett tidigare skede än vad som är fallet i dag utan en särskild registreringsskyldighet. En identitet kommer även att kunna etableras av svenska myndigheter – närmare bestämt Skatteverket – i samband med registreringsförfarandet, genom tilldelning av samordningsnummer. Enligt förslagen i nämnda betänkande ska Migrationsverket begära ett samordningsnummer hos Skatteverket för en EES-medborgare när han eller hon får ett registreringsbevis utfärdat. En identitetskontroll – med användning av biometriska uppgifter – kommer då normalt att göras av Skatteverket (se avsnitt 6.4.2). Begäran ska emellertid inte göras om EES-

[9] SOU 2026:9, s. 119.
[10] SOU 2026:9, s. 139, 158 f. och 194.

medborgaren är eller har varit folkbokförd eller redan har tilldelats ett samordningsnummer.[11]

6.3 Polismyndigheten

I Sverige ansvarar Polismyndigheten för gränskontrollerna, såväl vid yttre (mot ett land utanför EU/Schengen) som inre gräns (mot ett annat EU- eller Schengenland). Även om Tullverket och Kustbevakningen enligt lag är skyldiga att hjälpa Polismyndigheten vid en sådan kontroll och Kustbevakningen ska medverka till kontrollen genom att utöva kontroll av sjötrafiken har Polismyndigheten huvudansvaret. Polismyndigheteten ansvarar även för att kontrollera att personer som vistas i Sverige har rätt att göra det (inre utlänningskontroller).

6.3.1 Gränskontroller

Sverige ingår i Schengensamarbetet, vilket bland annat syftar till att uppnå målsättningen att upprätta ett område inom EU utan inre gränser med fri rörlighet för personer och därmed slopad personkontroll. Alla som passerar en yttre gräns och reser in i Sverige ska däremot genomgå en obligatorisk inresekontroll. Det huvudsakliga regelverket för gränspassage finns i gränskodexen. Kompletterande bestämmelser finns i 9 kap. utlänningslagen och i utlänningsförordningen (2006:97).

En utlänning som reser in i Sverige ska ha pass och av inresevillkoren för tredjelandsmedborgare i artikel 6 i gränskodexen följer att en grundförutsättning för inresa är att utlänningen är innehavare av en giltig resehandling. Gränskontrollen syftar bland annat till att kontrollera att inresevillkoren enligt artikel 6 i gränskodexen är uppfyllda. Av artikel 14.1 i gränskodexen framgår att en tredjelandsmedborgare som inte uppfyller samtliga inresevillkor som utgångspunkt ska nekas inresa. Med dessa bestämmelser som utgångspunkt krävs alltså för inresa i landet att identiteten är styrkt. Om personen ansöker om internationellt skydd kan inresa dock inte nekas enligt

[11] SOU 2026:9, s. 170.

gränskodexen, även om identiteten inte är styrkt eller ens har gjorts sannolik.

Omfattningen av kontrollen varierar beroende på om personen är EES-medborgare – och åtnjuter rätten till fri rörlighet – eller är tredjelandsmedborgare. Enligt artikel 8.2 i gränskodexen ska förstnämnda personkategori underkastas en grundläggande kontroll, som i första hand omfattar identitetskontroll samt kontroll av giltighet av resehandlingen för gränspassage samt sökning i relevanta databaser, bland annat Schengen Information System (SIS). För tredjelandsmedborgare gäller en mer noggrann kontroll, enligt artikel 8.3 i gränskodexen. Denna innefattar de åtgärder som nyss nämnts, men även en sökning i VIS för att kontrollera om personen är viseringspliktig och vissa kontrollfrågor. Vid gränskontroller verifierar Polismyndigheten alltså normalt sett identitet på personen i fråga genom att kontrollera rese- och tillståndshandlingar, men även andra metoder kan vara av betydelse i vissa fall, bland annat sökningar i EU-gemensamma informationssystem med stöd av gränsförordningen, in- och utreseförordningen och VIS-förordningen.

Gränskontroller aktualiserar i första hand ett behov av att kunna verifiera identitet, resehandlingar och tillstånd för vistelsen. Det är mer sällan fråga om att Polismyndigheten i samband med gränskontrollen behöver bestämma och registrera en grundidentitet.

6.3.2 Inre utlänningskontroller

En inre utlänningskontroll innebär en kontroll av en utlänning som finns inne i landet, i syfte att kontrollera utlänningens rätt att vistas här. Polismyndigheten har en generell befogenhet att vidta vissa utredningsåtgärder i syfte att kontrollera om en utlänning som vistas i landet saknar rätt att vistas här. Denna befogenhet är inte särskilt reglerad utan följer av myndighetens allmänna uppdrag att motverka olovlig vistelse. Myndighetens befogenhet att vidta vissa särskilda åtgärder vid en inre utlänningskontroll regleras emellertid i lag, huvudsakligen i 9 kap. utlänningslagen men även i lagen (2023:474) om polisiära befogenheter i gränsnära områden.

Enligt 9 kap. 9 § tredje stycket utlänningslagen får en inre utlänningskontroll endast vidtas om det finns grundad anledning att anta att utlänningen saknar rätt att uppehålla sig här i landet eller

om det annars finns särskild anledning till kontroll. De grundläggande kraven anger en allmän tröskel för när det anses vara motiverat att vidta en särskild kontrollåtgärd, exempelvis möjligheten att eftersöka och omhänderta pass och andra handlingar eller att fotografera utlänningen och ta hans eller hennes fingeravtryck. För att kunna verifiera identitet för eller identifiera en utlänning som påträffas i Sverige och är föremål för en inre utlänningskontroll kan Polismyndigheteten behöva vidta olika utredningsåtgärder. Kontroll av pass och andra identitetshandlingar är naturligtvis centralt, men även frågor till utlänningen och kontroller i EU-gemensamma informationssystem, eventuellt med hjälp av biometriska uppgifter, är betydelsefulla utredningsåtgärder. Stöd för detta finns i EU:s interoperabilitetsförordningar[12], VIS-förordningen, gränsförordningen och in- och utreseförordningen. En inre utlänningskontroll är till sin natur sådan att den genomförs vid ett tillfälle när utlänningen är personligen närvarande, men det finns även möjlighet att kräva att utlänningen inställer sig för utredning samt att hämta honom eller henne även utan föregående kallelse.

I likhet med gränskontroller aktualiserar inre utlänningskontroller i första hand ett behov av att kunna verifiera identitet samt kontrollera resehandlingar och tillstånd för vistelsen. Det är mer sällan fråga om att Polismyndigheten i samband med en inre utlänningskontroll behöver etablera en grundidentitet.

6.4 Skatteverket

Skatteverket ansvarar för folkbokföringsverksamheten i Sverige. Vid bland annat inflyttning till Sverige och i ärenden om tilldelning av samordningsnummer är Skatteverket den myndighet som bestämmer en grundidentitet.

[12] Europaparlamentets och rådets förordningar (EU) 2019/817 och (EU) 2019/818 av den 20 maj 2019.

6.4.1 Folkbokföring

De materiella bestämmelserna om folkbokföring finns i folkbokföringslagen (1991:481) och i folkbokföringsförordningen (1991:749).

Barn som föds levande i landet ska folkbokföras om modern är folkbokförd eller om fadern är folkbokförd och vårdnadshavare. För att bli folkbokförd i Sverige efter inflyttning krävs att personen anses vara bosatt i landet i folkbokföringslagens mening, vilket innebär att han eller hon kan antas komma att regelmässigt tillbringa dygnsvilan i landet under minst ett år. Även den som kan antas komma att regelmässigt tillbringa sin dygnsvila både inom och utom landet ska folkbokföras om han eller hon med hänsyn till samtliga omständigheter får anses ha sin egentliga hemvist här. En utlänning som måste ha uppehållsrätt eller uppehållstillstånd för att få vistas i Sverige får folkbokföras endast om detta villkor är uppfyllt eller om det finns synnerliga skäl för att han eller hon ändå ska folkbokföras.

Som huvudregel gäller att en inflyttande ska styrka identiteten för att kunna folkbokföras.[13] Den identitetskontroll som genomförs innan folkbokföring är av stor betydelse för att motverka att oriktiga uppgifter registreras i folkbokföringsverksamheteten. Bedömningen av en persons identitet utgör därmed en viktig del i ett sådant ärende. Vid födelse i Sverige krävs vanligtvis inte några mer omfattande utredningsåtgärder utan identiteten anses normalt styrkt utifrån de uppgifter som Skatteverket får från sjukhuset och som är tillgängliga om föräldrarna. Vid inflyttning till Sverige kan däremot fler utredningsåtgärder krävas. Skatteverkets prövning av om en person med uppehållstillstånd ska folkbokföras föregås dock av Migrationsverkets identitetsutredning och identitetsbedömning i uppehållstillståndsfrågan.[14] En grundidentitet har då ofta redan bestämts av Migrationsverket och kommer i många fall att ligga till grund för Skatteverkets bedömning. För EES-medborgare med uppehållsrätt kan utredningen om identiteten däremot behöva göras av Skatteverket i större utsträckning.

En person som anmäler inflyttning från utlandet ska, enligt huvudregeln, inställa sig personligen hos Skatteverket för identitetskontroll. Det framgår av 26 a § folkbokföringslagen. Identitetshandlingar spelar en avgörande roll vid Skatteverkets identitetskontroller i ärenden

[13] *Om folkbokföring, samordningsnummer och identitetsnummer*, SOU 2021:57, s. 193.
[14] *Ett säkert statligt ID-kort – med e-legitimation*, SOU 2019:14, s. 207.

om inflyttning till Sverige. Enligt 26 b och c §§ kan kontroller därför göras av de biometriska uppgifter som är lagrade i en identitetshandling. Skatteverket har också möjlighet att genom en begäran till Migrationsverket hämta in uppgifter från den centrala utlänningsdatabasen, med stöd av bestämmelsen i 7 kap. 15 b § utlänningsförordningen.

6.4.2 Tilldelning av samordningsnummer

Skatteverket fastställer ett personnummer som identitetsbeteckning för varje folkbokförd person. Det har emellertid blivit allt vanligare att personer vistas såväl kortare som längre perioder i Sverige, även om de inte är bosatta i landet i folkbokföringslagens mening. För personer som inte folkbokförs fastställs normalt inget personnummer. De kan i stället tilldelas ett samordningsnummer, vilket syftar till att tillgodose myndigheternas behov av ett enhetligt nummer för att utbyta information om personen och undvika personförväxling, men även till att tillgodose den enskildes behov av att ha en fungerande identitetsbeteckning för att kunna sköta sitt vardagliga liv.[15]

Samordningsnumret är konstruerat som ett personnummer men med sifferkombinationer som inte kan förekomma i ett personnummer. Siffrorna för dag adderas med 60. På motsvarande sätt som ett personnummer är ett samordningsnummer bestående och unikt, såtillvida att två identiska nummer inte förekommer och att det alltid är kopplat till en viss person, oavsett om denne lämnar landet eller avlider. Om en person med ett samordningsnummer senare blir folkbokförd ersätts numret däremot med ett personnummer.

Tilldelning av samordningsnummer regleras i lagen (2022:1697) om samordningsnummer och i förordningen (2023:363) om samordningsnummer. En person kan för det första tilldelas ett samordningsnummer på begäran av en sådan myndighet eller ett sådant annat organ som regeringen bestämmer. Det framgår av 2 kap. 1 § första stycket 1 lagen om samordningsnummer. Det är i dessa fall myndighetens behov av numret som styr om ett nummer ska tilldelas. En myndighet som begär ett samordningsnummer ska endast göra det som ett led i myndighetens handläggning av ett ärende och

[15] *Personnummer och samordningsnummer*, prop. 2008/09:111, s. 30.

inte som en fristående process inför en utlovad kommande ansökan.[16] Enskilda kan också tilldelas ett samordningsnummer efter en egen ansökan, under förutsättning att personen har en sådan anknytning till Sverige att han eller hon kan antas behöva en identitetsbeteckning (2 kap. 1 § första stycket 2). En sådan anknytning kan exempelvis vara att den enskilde eller någon annan i familjen äger eller innehar fast egendom, en tomträtt, en bostadsrätt eller en hyresrätt i Sverige.[17]

Huvudregeln är att den som ska tilldelas ett samordningsnummer ska styrka sin identitet, se 2 kap. 2 § lagen om samordningsnummer. Detta ska föregås av personlig inställelse för identitetskontroll. Vid en sådan kontroll ska pass eller annan identitetshandling och eventuellt uppehållstillståndskort som den enskilde innehar överlämnas på begäran av Skatteverket (3 §). Om en sådan handling innehåller biometriska underlag kan Skatteverket ta upp biometriska underlag för att jämföra dem med de som är lagrade i handlingen (4 §). Syftet med identitetskontrollen är att bedöma innehavarens identitet. Normalt sker identitetskontrollen vid Statens servicecenter.

Det kan också finnas behov av att tilldela personer ett samordningsnummer även om deras identitet inte kan styrkas. Personer som ska registreras i exempelvis belastningsregister, misstankeregister eller i övrigt inom rättsväsendets informationssystem har typiskt sett inte något intresse av att styrka sin identitet och det saknas ofta identitetshandlingar. För att rättsväsendet ska kunna hålla reda på dessa personer behövs en enhetlig personbeteckning även om identiteten inte kan fastställas.[18] Samordningsnummer kan därför enligt 5 § respektive 6 § tilldelas även när identiteten gjorts sannolik eller är osäker. Att den enskildes identitet har gjorts sannolik innebär att uppgifter om bland annat personens namn, födelsetid och medborgarskap har kunnat kontrolleras på något sätt även om identitetshandlingar inte personligen har överlämnats för kontroll, till exempel om personen har skickat in en kopia av en identitetshandling eller har inställt sig personligen för identitetskontroll men saknat handlingar av godtagbar kvalitet eller standard för att identiteten ska kunna bedömas vara styrkt.[19]

---

[16] SOU 2021:57, s. 365.
[17] *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, prop. 2020/21:160, s. 53.
[18] *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 25.
[19] Prop. 2021/22:276, s. 76, 89 och 140 f.

7 Verifiering av identitet och identifiering

7.1 Inledning

En persons identitet kan behöva verifieras i en mängd olika sammanhang, såväl av myndigheter som av privata aktörer. Verifiering kan behöva ske inom ramen för ett ärende då en grundidentitet bestäms, i syfte att säkerställa att personen är den som han eller hon utger sig för att vara. Polismyndigheten, Migrationsverket och Skatteverket har en central roll i sådana ärenden och har – som vi återkommer till nedan – en bred flora av rättsliga verktyg för att utreda och verifiera identitet i exempelvis ett ärende om uppehållstillstånd eller vid en inre utlänningskontroll. Verifiering behöver emellertid också ske i många andra sammanhang, mot en redan etablerad identitet. I våra direktiv anges att kopplingen till *grundidentitete*n behöver stärkas, men verifiering sker enligt vår mening rätteligen mot den identitet som en person gör gällande och är registrerad med vid en viss tidpunkt, vilket inte nödvändigtvis är grundidentiteten. Identiteten för en person är enligt vår mening inte statisk utan den initiala identiteten – grundidentiteten – som fastställs kan ändras över tid, av olika skäl. Till exempel kan en person som beviljas uppehållstillstånd i identitet A komma in med nya uppgifter om födelsetid i samband med en senare ansökan om naturalisation, och beviljas svenskt medborgarskap i den identiteten med utgångspunkt i den nya födelsetiden, det vill säga i identitet B; detta ska inte förstås som att personen har multipla identiteter, eftersom han eller hon endast är registrerad med *en* identitet, nämligen B. Identitet B är då den etablerade identiteten som individen är känd under och kan förväntas uppträda i. En annan vanligt förekommande situation är att någon byter efternamn i samband med äktenskap. Även om grundidentiteten ofta kan komma

att vara densamma för en person under hela vistelsen i Sverige utgår vår fortsatta analys från hur *identitet* kan verifieras i olika sammanhang, utan någon begränsning till grundidentitet.

Med detta sagt får etablering av grundidentiteten anses ha en särskilt viktig roll, då risken för att felaktiga, falska eller multipla identiteter etableras får antas vara som störst i detta skede. Som nämnts har Polismyndigheten, Migrationsverket och Skatteverket en central roll i identitetsförvaltningen genom att de ansvarar för att bestämma en grundidentitet för personer som av olika skäl vistas, eller vill vistas, i Sverige. Detta sker i första hand i samband med folkbokföring vid födelse i och inflyttning till Sverige, tilldelning av samordningsnummer och ansökan om visering eller uppehållstillstånd. En grundidentitet kan också i mer begränsad utsträckning behöva fastställas vid en gränskontroll eller en inre utlänningskontroll, eller vid registrering av en EES-medborgare. Förutom dessa ärenden kan vi konstatera att vid förvärv av svenskt medborgarskap genom naturalisation är utredningen av identiteten central. Beviljande av medborgarskap innebär också – i vart fall i teorin – att en ny identitet registreras för sökanden, genom att medborgarskapet ändras.

Fokus för redogörelsen i detta kapitel av hur identitet kan verifieras är på de ärenden som handläggs av Polismyndigheten, Migrationsverket och Skatteverket och som förutsätter att identiteten utreds och kontrolleras närmare. Detta inkluderar ärenden om utfärdande av rese- eller identitetshandlingar. Fokus för vårt uppdrag är dock att stärka kopplingen mellan en etablerad identitet och verifiering av identiteten, med grund i biometriska uppgifter. Befintliga möjligheter att verifiera identitet i andra situationer kommer därför också att nämnas i detta kapitel; att lämna en mer heltäckande redogörelse för alla tänkbara situationer är emellertid inte möjligt.

I avsnitt 7.2 beskriver vi vad som menas med verifiering av identitet och hur det förhåller sig till beviskrav som kan förekomma i ett ärendeslag. Det kan också vara så att en person av olika anledningar inte kan eller vill medverka till att klarlägga sin identitet och att en verifiering inte kan genomföras. Personen kan då behöva identifieras. Vad som avses med detta begrepp och vilka möjligheter som finns att identifiera en person beskriver vi i avsnitt 7.3. I avsnitt 7.4 redogör vi för vilka metoder för att verifiera identitet som kan användas och vilket gällande, beslutat och föreslaget rättsligt stöd som finns i vissa situationer. När det gäller redogörelsen av vilka olika åtgärder

för att verifiera identitet eller identifiera en person som kan aktualiseras syftar den till att ge en översiktlig bild. De aktuella regelverken, i synnerhet de EU-förordningar som är tillämpliga på utlänningsrättens område, är mycket omfattande. Att i detalj redogöra för hur dessa ska tillämpas, eller vilka närmare åtgärder som ska eller bör vidtas i ett visst enskilt fall, är inte möjligt i detta sammanhang. Det är inte heller nödvändigt för att uppnå syftet med redogörelsen i detta kapitel, som i första hand är att tjäna som utgångspunkt för våra vidare övervändanden av vilka åtgärder som är lämpliga för att stärka möjligheten att verifiera identitet med grund i biometriska uppgifter.

7.2 Verifiering av identitet

Verifiering av identitet syftar till att besvara frågan *Är personen den som han eller hon utger sig för att vara?* Det behöver alltså fastställas en koppling mellan den fysiska personen som myndigheten har kontakt med och de identitetsuppgifter som han eller hon uppger, eller som myndigheten på något annat sätt har fått fram.

Verifiering avser alltså inte att bekräfta identitetsuppgifternas tillförlitlighet i sig eller att avgöra om ett visst beviskrav är uppfyllt. Samtidigt kan ett behov av att verifiera identiteten ofta aktualiseras just i ärenden där det finns ett beviskrav kopplat till identitet, exempelvis genom att det av 11 och 12 §§ lagen (2001:82) om svenskt medborgarskap (medborgarskapslagen) framgår att det som utgångspunkt krävs att identiteten är styrkt för att en utlänning ska kunna beviljas svenskt medborgarskap. Det är då av stor vikt att klarlägga att personen också är den som hon han eller hon utger sig för att vara. I ett ärende där något beviskrav inte ställs upp eller där andra faktorer är avgörande kan verifiering av identitet vara av underordnad betydelse. En verifiering av identitet aktualiseras i många fall på initiativ av den enskilde genom att han eller hon ansöker om något – till exempel en Schengenvisering, ett svenskt medborgarskap eller ett svenskt pass – men kan även behöva göras i samband med att företrädare för en myndighet påträffar en person och behöver utreda vem han eller hon är. Ett exempel på sistnämnda situation är de inre utlänningskontroller som Polismyndigheten genomför.

7.2.1 Närmare om begreppet verifiering

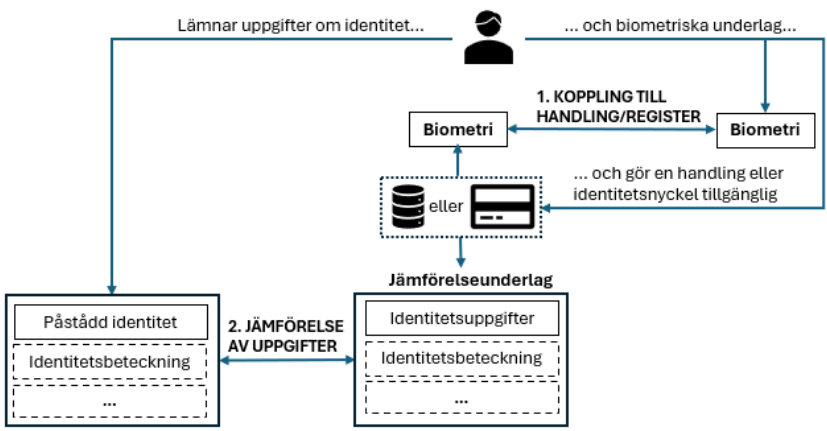
Vår definition

Med *verifiering av identitet* avses i detta betänkande att en grupp av uppgifter jämförs med en annan, för att fastställa om en påstådd identitet är riktig, så kallad en-till-en-jämförelse. Om biometriska uppgifter används vid jämförelsen är det fråga om *biometrisk verifiering av identitet*.

Det finns inte någon legaldefinition i svensk rätt av vad som avses med verifiering av identitet, men begreppet återfinns i flera av de EU-förordningar som är aktuella på utlänningsrättens område. I exempelvis artikel 3.13 i in- och utreseförordningen[1] definieras *verifiering* som förfarandet att jämföra en uppsättning uppgifter med en annan för att fastställa om en påstådd identitet är den riktiga.

Verifiering av identitet genomförs som vi ser det i praktiken i två steg: dels en jämförelse mellan den påstådda identiteten och de identitetsuppgifter som utgör jämförelseunderlag, dels en koppling mellan sistnämnda underlag och den individ vars identitet ska verifieras, exempelvis med hjälp av biometriska uppgifter. Detta kan schematiskt illustreras på följande sätt.

Figur 7.1 Biometrisk verifiering av identitet



[1] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.

Uppgifter om den påstådda identiteten kan komma myndigheten tillhanda exempelvis genom att de anges i en ansökan eller framgår av en handling som den enskilde lämnar över. Det är som vi ser det inte nödvändigt att identitetsuppgifterna som utgör den påstådda identiteten är direkt synliga för handläggaren vid myndigheten vid verifieringstillfället, utan det är tillräckligt att de finns indirekt tillgängliga, exempelvis genom att de är knutna till ett person- eller samordningsnummer som den enskilde anger och är registrerade i något system hos myndigheten eller som den har tillgång till; exempelvis kan uppgifterna finnas lagrade i folkbokföringsverksamheten eller den centrala utlänningsdatabasen.

När det gäller de uppgifter som kan utgöra jämförelseunderlag i ett visst fall framgår dessa normalt sett av en identitetshandling eller finns sparade i ett register. Exempel på sådana register är den centrala utlänningsdatabasen och centrala informationssystem inom EU, om ett sådant är tillgängligt i det enskilda ärendeslaget. Som exempel på sistnämnda register kan nämnas in- och utresesystemet och EU:s gemensamma databas för identitetsuppgifter, CIR; en kontroll mot detta register är obligatorisk i vissa situationer, bland annat vid en gränskontroll (se artikel 23.2 i in- och utreseförordningen) och när en tredjelandsmedborgare ansöker om internationellt skydd (se artikel 8.5 och 14 i screeningförordningen[2]). I avsnitt 7.4.3 återkommer vi till vilka register som kan aktualiseras i de ärenden som Polismyndigheten, Migrationsverket och Skatteverket handlägger, där någons identitet behöver verifieras. Det kan även tänkas att ett jämförelseunderlag utgörs av muntliga uppgifter från någon som intygar att den påstådda identiteten är korrekt. Tillförlitligheten i ett sådant underlag får enligt vår mening dock anses låg. Det saknas som vi ser det hinder mot att flera olika jämförelseunderlag används.

För att en jämförelse mellan den påstådda identiteten och uppgifter som i ett enskilt fall utgör jämförelseunderlag ska kunna göras på ett tillförlitligt sätt behöver dock först en koppling etableras mellan den vars identitet ska verifieras och ett visst jämförelseunderlag. Kopplingen kan göras på olika sätt. Om de identitetsuppgifter som utgör jämförelseunderlag har hämtats från en identitetshandling kan en okulär kontroll göras mellan ansiktsbilden på handlingen och personen som myndigheten möter (se avsnitt 7.4.2). En mer tillförlitlig metod är – som vi återkommer till i nyss nämnda avsnitt

[2] Europaparlamentets och rådets förordning (EU) 2024/1356 av den 14 maj 2024.

och i avsnitt 7.4.3 – att använda biometriska uppgifter som kan tas fram ur handlingen eller som finns lagrade i ett register och jämföra dem med de som kan tas fram ur en ansiktsbild eller fingeravtryck som tas upp från den enskilde. En jämförelse som görs med hjälp av biometriska uppgifter är den metod som ska tillämpas enligt flera av de EU-förordningar som aktualiseras vid bland annat gränskontroller, inre utlänningskontroller och ansökan om uppehållstillstånd. Metoden har ett brett spektrum av praktiska tillämpningar. På flygplatser kan till exempel utökad automatisering av verifiering av identitet minska väntetiderna för säkerhets- och incheckningsprocedurer. Om ett centralt register används vid verifieringen kommer normalt sett de identitetsuppgifter som utgör den påstådda identiteten, eller andra uppgifter som lämnats av den enskilde eller som på annat sätt tagits fram i ärendet, att användas för att genom en alfanumerisk[3] sökning mot hela databasen lokalisera en lagrad individ som matchar dessa; de biometriska uppgifter som är knutna till träffen kan därefter användas för att etablera en tillförlitlig koppling mellan de jämförelseuppgifter i fråga om identitet som finns lagrade i registret och individen. Även andra typer av uppgifter som kan vara knutna till den träff som har lokaliserats i ett register kan användas för att etablera en koppling. Till exempel kan en ansiktsbild som finns lagrad i den centrala utlänningsdatabasen i ett ärende jämföras okulärt med den person som ansöker om uppehållstillstånd. Det kan även tänkas att sidouppgifter av annat slag som finns lagrade i databasen jämförs med information som lämnats av den enskilde i ärendet eller som annars förekommer i ärendet, även om detta är mindre tillförlitligt. Det kan exempelvis röra sig om identitetsbeteckningar eller uppgifter om kön.

Huruvida en tillförlitlig koppling mellan en påstådd identitet och ett visst jämförelseunderlag kan göras får avgöras utifrån omständigheterna i det enskilda fallet. Om biometriska uppgifter används avgörs detta ofta utifrån en datorstödd jämförelse, mot vissa angivna tröskelvärden. Under förutsättning att en koppling kan anses ha etablerats, och den påstådda identiteten och de identitetsuppgifter som utgör jämförelseunderlag också stämmer överens, kan myndigheten anses ha fått svar på om den påstådda identiteten är riktig,

[3] I artikel 3.15 i in- och utreseförordningen definieras detta begrepp som uppgifter som återges med bokstäver, siffror, särskilda tecken, mellanslag och skiljetecken. Vi använder begreppet i denna betydelse i betänkandet.

och därmed på den initiala frågan: *är personen den som han eller hon utger sig för att vara?*

Om en koppling däremot inte har kunnat göras – exempelvis på grund av att en sökning med alfanumeriska uppgifter har resulterat i flera träffar, eller de biometriska uppgifter som finns lagrade för en viss träff i ett register eller i en viss handling inte matchar de som tagits fram på plats – kan en *identifiering* av personen behöva göras, för att identiteten hos den enskilde ska kunna verifieras. Vad detta innebär redogör vi för i avsnitt 7.3.

Verifiering av identitet innebär alltså, som vi ser det, att en grupp av uppgifter jämförs med en annan; som anfört ovan behöver i praktiken två jämförelser, av två olika grupper av uppgifter, genomföras. Detta förändrar som vi ser det dock inte definitionen av begreppet i sig. När vi i detta betänkande talar om verifiering av identitet avser detta – om inte annat särskilt anges – båda stegen. Om kopplingen i det första steget görs med hjälp av biometriska uppgifter anser vi att det är fråga om att *biometriskt verifiera identitet* (jfr avsnitt 23.5.5 angående detta begrepp).

7.2.2 Verifiering i förhållande till beviskrav

Vår bedömning

Att ett visst beviskrav avseende identiteten i ett ärende är uppfyllt innebär inte automatiskt att det går att bekräfta att den påstådda identiteten är riktig.

En viktig del i att kunna stärka identitetsförvaltningen är att identiteten för personer som vistas i Sverige kan bestämmas med så stor visshet som möjligt, utifrån ett tillförlitligt uppgiftsunderlag. Beroende på ärendeslaget kan olika beviskrav, som utgör måttet på vissheten, komma att tillämpas.

Beviskraven är ofta mer oklara och splittrade inom förvaltningsrätten än när det gäller brottmål och tvistemål av olika slag. En orsak är att förvaltningsprocessen innehåller mål av många olika slag som medför olika lösningar av såväl frågan om bevisbörda som kraven på bevisningens styrka (jfr HFD 2013 ref. 61 och HFD 2019 ref. 9). När det gäller identitet används huvudsakligen begreppet *styrkt*,

såväl i författning som i rättstillämpningen; även *klarlagd* och *fastställd* används men ger uttryck för ett och samma beviskrav (se MIG 2016:6). Ett annat beviskrav som förekommer exempelvis vid en ansökan om svenskt medborgarskap (se 12 § andra stycket medborgarskapslagen) är *sannolik*, vilket beskriver ett medelhögt beviskrav. Ett annat exempel där styrkt identitet inte krävs är vid prövning av en ansökan om internationellt skydd, med hänsyn till de bevissvårigheter som kan finnas i sådana ärenden.

Vi anser att det är viktigt att bedömningen av om ett beviskrav är uppfyllt inte blandas samman med verifiering av identiteten. Om ett visst beviskrav är uppfyllt eller inte har i första hand betydelse för utgången i ett visst ärende och svarar inte i sig på frågan om den person som myndigheten möter också är den som han eller hon utger sig för att vara; att personen kan anses ha uppfyllt det beviskrav som gäller i ett visst ärende behöver inte nödvändigtvis innebära att det har gått att bekräfta detta, i synnerhet om ett lägre beviskrav än styrkt tillämpas. Det kan även vara fråga om att identitetshandlingar har lånats ut eller framställts i fel identitet, vilket inte alltid kan upptäckas med lätthet; handlingen i sig kan vara äkta men uppgifterna i den avse någon annan person. Detta innebär alltså att även om myndigheten anser att beviskravet i ärendet är uppfyllt kan identiteten behöva *verifieras*, för att säkerställa att identiteten också kan knytas till den individ som gör den gällande. En sökning i ett register med alfanumeriska identitetsuppgifter är inte heller beroende av om identiteten är styrkt eller inte. Att sökningen ger en träff, som matchar de identitetsuppgifter som den enskilde gjort gällande, betyder alltså inte ensamt att myndigheten har fått svar på om personen är den som han eller hon utger sig för att vara, utan verifieringen av identiteten görs genom en en-till-en-jämförelse mot andra uppgifter kopplade till träffen, på det sätt vi beskrivit i avsnitt 7.2.1. Användning av biometriska uppgifter är då det säkraste sättet. Vi redogör i avsnitt 7.4.3 för vilka sökningar som får, eller i vissa ärendeslag ska, göras.

7.3 Identifiering

Att identifiera någon syftar till att besvara frågan Vem är du? Målet med en identifiering är att hitta en enda matchning i en databas utan att den enskilde aktivt måste, eller har kunnat, verifiera sin identitet. Det kan exempelvis vara fråga om ett ansiktsigenkänningssystem vid en konsert eller vid inpassering till en byggnad.

I de ärenden där Polismyndigheten, Migrationsverket och Skatteverket möter en person kan identifiering typiskt sett aktualiseras först när tillförlitligt underlag som kan användas för att verifiera identiteten saknas, eller när identiteten i övrigt är oklar. Det går då ofta inte att göra en en-mot-en-kontroll av en påstådd identitet. Ett exempel är att en utlänning påträffas av polis i landet och blir föremål för en inre utlänningskontroll, men saknar identitetshandlingar eller inte vill medverka till att lämna information om sin identitet. Att i denna situation kunna identifiera personen är viktigt för att kunna klarlägga om han eller hon har rätt att vistas i Sverige och i förlängningen upprätthålla en reglerad invandring. Det kan också vara viktigt för att kunna skydda barn och unga som uppehåller sig i Sverige utan att ansöka om uppehållstillstånd eller som avvikit från boenden de placerats på som ensamkommande barn.[4] En identifiering kan också behöva göras när en sökning i en databas med alfanumeriska uppgifter – vilka i sig kan vara styrkta – har gett flera träffar. Detta eftersom identiteten omfattar namn, födelsetid och medborgarskap – uppgifter som kan vara desamma för flera individer utan att för den delen vara falska eller felaktiga (se avsnitt 3.2).

7.3.1 Närmare om begreppet identifiering

Vår definition

Med *identifiering* avses i detta betänkande en sökning i ett register med hjälp av biometriska uppgifter, för att avgöra om den person som myndigheten möter förekommer i registret med någon identitet, det vill säga en en-till-många-jämförelse.

[4] *Vissa identitetsfrågor inom utlänningsrätten*, prop. 2020/21:159, s. 10.

Det saknas en legaldefinition av begreppet *identifiering* i svensk rätt. Begreppet förekommer däremot i olika sammanhang; till exempel framgår av artikel 4.14 i dataskyddsförordningen[5] att biometriska uppgifter möjliggör eller bekräftar identifieringen av en fysisk person och i likhet med verifiering återfinns begreppet i flera av de EU-förordningar som är aktuella på utlänningsrättens område. Som exempel kan nämnas artikel 3.14 i in- och utreseförordningen, som definierar identifiering som förfarandet att fastställa en persons identitet genom en databassökning mot flera grupper av uppgifter, men även artikel 3.35 i AI-förordningen[6] som anger att *biometrisk identifiering* innebär en jämförelse av upptagna biometriska uppgifter med biometriska uppgifter om enskilda personer som lagrats i en databas. Enligt bestämmelsen i 9 kap. 8 f § utlänningslagen (2005:716) kan fingeravtryck och fotografi tas upp för att genom en sökning i Schengens informationssystem (SIS) identifiera en utlänning, om identiteten inte kan fastställas på annat sätt.

Identifiering innebär alltså att en sökning görs mot en större uppsättning uppgifter i ett register för att avgöra om individen förekommer med någon identitet[7], en en-till-många-jämförelse Detta är en avgörande skillnad mot verifiering, som är en en-till-en-jämförelse mellan olika grupper av uppgifter. Att söka i ett register med alfanumeriska uppgifter i form av ett personnummer eller identitetsuppgifter som lämnats av den enskilde eller som framgår av en identitetshandling, i syfte att få en träff som kan användas för att biometriskt verifiera identitet, kan därmed också i sig anses utgöra en form av identifiering. När identiteten är oklar behöver identifiering i stället göras genom att biometriska uppgifter används i det första steget. Sökningar med hjälp av biometriska uppgifter pekas i flera EU-förordningar på utlänningsrättens område ut som ett sätt att bidra till en korrekt identifiering av personer. Sökningar baserade på biometriska uppgifter bidrar till en hög tillförlitlighet i jämförelsen och främjar möjligheten att lokalisera en unik träff som kan ligga till grund för verifiering av identiteten. Mot denna bakgrund avser vi med begreppet identifiering, i detta betänkande, endast en-till-många-jämförelser med hjälp av biometriska uppgifter.

[5] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[6] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni.
[7] *Anpassning av svensk rätt till den reviderade VIS-förordningen*, Ds 2023:30, s. 54.

7.3.2 Möjlighet att identifiera en person i olika sammanhang

Att kunna identifiera någon utifrån biometriska uppgifter är, särskilt i ärenden där en grundidentitet kan behöva etableras, en betydelsefull åtgärd för att klarlägga vem en person är när identiteten inte kan bekräftas på annat sätt. Det finns därför ett förhållandevis brett stöd för detta i flera EU-förordningar. Framför allt kan artikel 23.4 och 27 i in- och utreseförordningen, artikel 19.3, 20 och 22i i VIS-förordningen[8] och artikel 33.2 i gränsförordningen[9] nämnas. Förordningarna ger samtliga en möjlighet att identifiera en tredjelandsmedborgare vid gränskontroller och inre utlänningskontroller. VIS-förordningen är mer begränsad i dessa ärenden, då den endast omfattar – och ska omfatta – tredjelandsmedborgare som innehar visering eller uppehållstillstånd. Med stöd av gränsförordningen kan även personer som ansöker om internationellt skydd identifieras, och i tillståndsärenden kan tredjelandsmedborgare som inte omfattas av rörlighetsdirektivet identifieras enligt in- och utreseförordningen. Utöver nämnda förordningar ger artikel 20 och 20a i EU:s förordningar om interoperabilitet[10] stöd för att kunna identifiera tredjelandsmedborgare respektive personer som ansöker om internationellt skydd, i det senare fallet med stöd av artikel 14.2 i screeningförordningen. Nämnda förordningar innehåller, utöver artikel 9.2 i screeningförordningen som hänvisar till Eurodacförordningen[11], inte ett uttryckligt stöd för att ta upp de biometriska underlag som ligger till grund för identifieringen. Kompletterande bestämmelser finns därför införda i 9 kap. utlänningslagen. Personkretsen som omfattas i dessa bestämmelser i utlänningslagen är i viss mån begränsad, genom att gällande och föreslagna bestämmelser endast ger stöd för att ta fingeravtryck om utlänningen har fyllt sex år eller, när det gäller identifiering enligt artikel 27 i in- och utreseförordningen, tolv år (angående sistnämnda fall, se 9 kap. 8 d § utlänningslagen).

Migrationsverkets register över fingeravtryck och fotografier ger även vissa möjligheter att kunna identifiera en person vid en inre utlänningskontroll eller en ansökan om uppehållstillstånd. Vid en inre utlänningskontroll har Polismyndigheten, enligt bestämmelsen

[8] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008.
[9] Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018.
[10] Europaparlamentets och rådets förordningar (EU) 2019/817 och (EU) 2019/818 av den 20 maj 2019.
[11] Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013.

i 9 § utlänningsdataförordningen (2016:30) och 19 § utlänningsdatalagen (2016:27), direktåtkomst till personuppgifter hos Migrationsverket, och av bestämmelsen i 15 § 6 utlänningsdatalagen framgår att fingeravtryck och fotografier i verkets register får användas vid inre utlänningskontroller. I ärenden om uppehållstillstånd som grundar sig på ett skyddsbehov kan Migrationsverket genomföra sökningar i det egna registret utlänningsdatabasen. Fingeravtryck får även kontrolleras mot det biometriregister som Polismyndigheten för. Detta framgår av 15 § 1 respektive 5 utlänningsdatalagen och 5 kap. 1 § 5 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Det kan i detta sammanhang noteras att förslag har lagts om att 15 § 1 utlänningsdatalagen ska ändras så att den avser samtliga ärenden om uppehållstillstånd.[12] I propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* har föreslagits att Migrationsverket ska kunna jämföra biometriska uppgifter som tas fram i ärenden med stöd av 9 kap. 8 § utlänningslagen mot sådana uppgifter som, enligt de förslag som lämnats av regeringen i andra delar, ska få lagras hos Skatteverket.[13] När det gäller ärenden om inflyttning till Sverige och tilldelning av samordningsnummer har förslag lämnats på bestämmelser som ska möjliggöra att biometriska uppgifter används för att identifiera en person. Det kan inte utläsas att förslagen innehåller någon begränsning som innebär att de endast skulle avse tredjelandsmedborgare.[14]

Nedan ges en översikt av när identifiering med hjälp av biometriska uppgifter kan göras i olika sammanhang. De bestämmelser som anges i tabellen avser utlänningslagen om inte annat särskilt anges. Bestämmelser som är kursiverade avser lämnade förslag.

[12] *Stärkt återvändandeverksamhet*, prop. 2025/26:263, s. 182 f. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.
[13] *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten*, prop. 2025/26:261, s. 81.
[14] Prop. 2025/26:261, s. 103 f. och 114 f.

Tabell 7.1 Identifiering med hjälp av biometriska uppgifter

Vid…	… kan jämförelse göras med uppgifter i	… med biometriska uppgifter som tagits upp enligt
Gränskontroll	SIS	9 kap. 8 f § och 9 kap. 8 § 1
	VIS, In- och utresesystemet	9 kap. 8 d §
	CIR	9 kap. 8 § 2
Inre utlänningskontroll	SIS	9 kap. 8 f §
	VIS	*9 kap. 8 h §*[1]
	In- och utresesystemet	9 kap. 8 h §
	CIR	*9 kap. 8 j §*[2]
	Migrationsverkets register över fingeravtryck och fotografier	9 kap. 8 § 4
Uppehållstillstånd	SIS och CIR (skyddsbehov)	9 kap. 8 § 2 och 8 a §
	In- och utresesystemet (tillståndsärenden)	9 kap. 8 a § fjärde stycket
	Migrationsverkets register över fingeravtryck och fotografier	9 kap. 8 § 2
	Polismyndighetens biometriregister	9 kap. 8 § 2
	Uppgifter i folkbokförings-verksamheten	*15 § 14 utlänningsdatalagen*[3]
Av- och utvisning	SIS	9 kap. 8 § 5
Schengenvisering	VIS	Artikel 13 i viseringskodexen[4]
Nationell visering	VIS	*9 kap. 8 j §*[5]
Inflyttning till Sverige	Uppgifter i folkbokförings-verksamheten	*26 d § andra stycket folkbokföringslagen*[6]
	Migrationsverkets register över fingeravtryck och fotografier	*26 e § första stycket folkbokföringslagen*[7]
Tilldelning av samordningsnummer	Uppgifter i folkbokföringsverksamheten	*2 kap. 4 a § lagen om samordningsnummer*[8]
	Migrationsverkets register över fingeravtryck och fotografier	*2 kap. 4 b § lagen om samordningsnummer*[9]

[1] Anpassning av svensk rätt till den reviderade VIS-förordningen, prop. 2024/25:176, s. 55.

[2] Anpassningar av svensk rätt till EU:s förordningar om interoperabilitet, Ds 2022:21, s. 89. Förslag på en bestämmelse i 8 j § finns även i prop. 2024/25:176.

[3] Prop. 2025/26:261, s. 110. Med den ordning som föreslås i prop. 2025/26:263 kommer Migrationsverket att kunna göra en sökning i alla ärenden om uppehållstillstånd och även vid ansökan om svenskt medborgarskap.

[4] Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009.

[5] Prop. 2024/25:176, s. 35 f.

[6] Prop. 2025/26:261, s. 103.

[7] Prop. 2025/26:261, s. 103 f.

[8] Prop. 2025/26:261, s. 114.

[9] Prop. 2025/26:261, s. 115.

Utöver vad som framgår av tabellen ovan saknas, såvitt vi har kunnat finna, stöd för myndigheter eller andra aktörer för att – utanför den brottsbekämpande verksamheten – identifiera personer, i den mening som avses i detta betänkande, det vill säga genom en en-till-många-jämförelse med biometriska uppgifter.

Om sökningen med biometriska uppgifter ger en träff har personen identifierats. Det kan normalt antas att den träff i databasen som lokaliserats också innehåller identitetsuppgifter och andra uppgifter, exempelvis om resehandlingar eller tidigare beslut om nekad inresa. Exempelvis vid en sökning som görs med stöd av EU:s förordningar om interoperabilitet ska polismyndigheterna, vid en träff som erhållits med hjälp av biometriska uppgifter, ha tillgång till uppgifter i CIR om identiteten (se artikel 20.3). Under förutsättning att det är fråga om en enda träff och det i övrigt inte finns motstridiga uppgifter om identiteten kan identiteten på detta sätt ofta anses indirekt ha verifierats. En manuell kontroll är dock nödvändig.

7.4 Metoder för att verifiera identitet

Som vi nämnt i avsnitt 7.2.1 finns det flera möjliga metoder som kan användas för att utreda och verifiera identitet. Beroende på i vilket ärendeslag som en myndighet eller annan aktör möter den enskilde kan olika metoder aktualiseras i varierande utsträckning. I frånvaro av närmare reglering av vilka metoder som får eller ska tillämpas i ett visst ärende gäller, för svenska myndigheter, som utgångspunkt den generella utredningsskyldighet som följer av 23 § förvaltningslagen (2017:900), nämligen att en myndighet ska se till att ett ärende blir utrett i den omfattning som dess beskaffenhet kräver. Syftet med utredningen är att klarlägga de för ärendet relevanta faktiska förhållandena. Utredningen ska genomföras på ett objektivt sätt och kraven på omfattningen av myndighetens utredningsåtgärder kan variera med hänsyn till ärendets karaktär.

7.4.1 Identifiering som metod för att verifiera identitet

Som noterats ovan kan identifiering användas utan att det krävs någon aktiv åtgärd från den enskilde sida, i vart fall om ansiktsbilder används vid jämförelsen. Om den myndighet som vill verifiera iden-

titet skulle kunna använda biometriska uppgifter för att identifiera en person genom en databassökning, och därmed också indirekt verifiera identiteten vid en träff, uppkommer därför frågan om denna metod kan eller bör användas direkt, utan att andra utredningsåtgärder först vidtagits. I betänkandet *Tidsbegränsat uppehållstillstånd vid oklar identitet och resväg* anfördes bland annat att problemen med att personer inte medverkar till att klarlägga sin identitet påverkar såväl myndigheter som sökande i allmänhet på så sätt att allt för stor andel av samhällets resurser används för att utreda identiteter och att ett sådant resursslöseri är av ondo och måste motverkas.[15] Att stora resurser kan behöva läggas ner på att utreda utlänningens hemvist och resväg för att försöka utröna gentemot vilket land eventuella skyddsskäl ska prövas, när handlingar som kan styrka identiteten saknas, uppmärksammades även av Återvändandeutredningen.[16] En eventuellt tidskrävande utredning av identiteten skulle alltså potentiellt kunna undvikas genom att biometriska uppgifter används tidigt i utredningen för att identifiera en person och på det sättet få fram uppgifter om en tidigare registrerad identitet.

En identifiering innebär – som vi anfört i avsnitt 7.3.1 – att en sökning görs mot en större uppsättning poster i en databas med biometriska uppgifter, vilket i ett dataskyddsperspektiv utgör behandling av känsliga personuppgifter. Särskilda begränsningar gäller för behandlingen av sådana uppgifter och sökningar med biometriska uppgifter medför uppenbara risker för den enskildes integritet.[17] Det är enligt vår mening viktigt att biometriska uppgifter inte används på ett sätt som innebär ett omotiverat intrång i den personliga integriteten. Som utgångspunkt bör därför en restriktiv hållning intas. Vi kan konstatera att en ordning som innebär att identifiering kan göras först när det inte går att verifiera identiteten på annat sätt – det vill säga genom kontroll mot innehållet i en identitetshandling eller en alfanumerisk sökning och efterföljande verifiering genom en en-till-en-jämförelse med hjälp av biometriska uppgifter – tillämpas i bland annat artikel 23.4 och 27 i in- och utreseförordningen, artikel 19.3, 20 och 22i i VIS-förordningen och artikel 33.2 i gränsförordningen. Att behandling av biometriska uppgifter bör minimeras får även stöd i de uttalanden som gjordes i samband med att anpassningar

[15] SOU 2004:132, s. 54.
[16] *Klarlagd identitet – Om utlänningars rätt att vistas i Sverige, inre utlänningskontroller och missbruk av identitetshandlingar*, SOU 2017:97, s. 67.
[17] Se exempelvis *Fingeravtryck i pass*, prop. 2008/09:132, s. 13.

gjordes i svensk rätt på grund av ändringar i SIS-regelverket; regeringen anförde bland annat att fotografier och fingeravtryck alltid får användas för att bekräfta identiteten på en person som har lokaliserats efter en alfanumerisk sökning i SIS, men att om identiteten kan bekräftas utan att använda biometriska uppgifter ska de inte heller användas.[18]

Mot denna bakgrund anser vi att utgångspunkten vid verifiering av identitet bör vara att identifiering med hjälp av biometriska uppgifter används först om det inte är möjligt att på annat sätt verifiera identiteten.

7.4.2 Verifiering av identitet mot handlingar

I flera av de ärendeslag där Polismyndigheten, Migrationsverket och Skatteverket har att verifiera identitet för någon förutsätts som utgångspunkt att personen kan styrka sin identitet, exempelvis för att kunna beviljas ett uppehållstillstånd eller tillåtas att resa in i landet. Identiteten styrks normalt genom att den enskilde överlämnar en giltig identitetshandling i form av ett pass, utfärdat av behörig myndighet i hemlandet, i original. Handlingen ska vara tillförlitlig och utfärdad på ett ur identitetssynpunkt tillfredsställande sätt.[19] Också i andra situationer sker verifieringen genom att den enskilde visar upp fysiska identitetshandlingar och att innehållet i dem kontrolleras, exempelvis en synlig ansiktsbild eller andra biometriska underlag. Detta kan bygga på uttryckliga krav i den lagstiftning som reglerar ett visst ärendeslag eller ha civilrättsliga grunder. Exempel på förstnämnda situationer är ansökan om pass eller nationellt identitetskort; av bestämmelsen i 3 kap. 2 § Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort (PMFS 2021:3) framgår att en sökande vid ansökningstillfället i första hand ska styrka sin identitet genom att visa upp en godtagbar identitetshandling. Ett exempel på verifiering av identitet på civilrättsliga grunder är krav på att den som hämtar ut ett paket ska kunna legitimera sig, genom att visa upp en godkänd identitetshandling.[20]

En verifiering av identitet kommer i dessa fall i första hand att ske genom en jämförelse av de uppgifter som den enskilde lämnat

[18] *Ändrade bestämmelser om fotografier och fingeravtryck i SIS II-regelverket*, prop. 2020/21:6, s. 16.
[19] Jfr *Medborgarskap och identitet*, prop. 1997/98:178, s. 8 och MIG 2010:17.
[20] https://www.postnord.se/privat/ta-emot/hamta/legitimering, hämtat den 19 maj 2026.

och de som framgår av identitetshandlingen, i kombination med en okulär jämförelse mellan ansiktsbilden på handlingen och den enskilde. I vissa fall kommer de identitetsuppgifter som framgår av handlingen också i praktiken vara de enda som så att säga har lämnats av den enskilde, genom att handlingen konkret har överlämnats, exempelvis till polis vid en inre utlänningskontroll. Någon egentlig jämförelse med andra uppgifter om identiteten sker i så fall inte, utan det är i stället själva innehavet av handlingen som kan sägas utgöra ett påstående om att den enskilde har en viss identitet. För att en handling på ett tillförlitligt sätt ska kunna verifiera innehavarens identitet behöver normalt kontroller göras av om den är äkta och om den är utfärdad till innehavaren. I detta avsnitt beskriver vi översiktligt hur detta går till och vilka åtgärder som myndigheter kan vidta i olika situationer. Som nämnts ovan är redogörelsen inriktad på ärenden där en grundidentitet kan behöva etableras. Även ärendeslag där en identitetshandling utfärdas av svenska myndigheter behandlas.

Handlingen behöver vara tillgänglig

En grundläggande förutsättning för att kunna använda en handling för att verifiera identitet är att myndigheten eller aktören i fråga har tillgång till den, som utgångspunkt i original; i MIG 2009:7 uttalade Migrationsöverdomstolen att i alla ärenden om tidsbegränsat uppehållstillstånd där den sökande omfattas av ett krav på pass ska passet visas upp i original. Syftet med att en passhandling ska visas upp i original är att möjliggöra en högre grad av kontroll av dess äkthet och minska risken för oegentligheter.

Att handlingen ska visas upp för myndigheten i original innebär indirekt att den enskilde behöver inställa sig personligen. I annat fall är det normalt sett inte möjligt att jämföra fotografiet på handlingen med personen eller de biometriska uppgifter som kan tas fram ur biometriska underlag som finns lagrade i handlingen med de som tas upp på plats[21], vilket vi återkommer till nedan. Det finns även uttryckliga lagkrav på personlig inställelse för att lämna över identitetshandlingar, bland annat i ärenden om folkbokföring vid inflyttning från utlandet och i ärenden om tilldelning av samordningsnummer

[21] För vissa personkategorier kan en digital passkontroll göras i ärenden om uppehållstillstånd för studier eller arbete, genom att sökanden, med hjälp av en särskild mobilapplikation tar ett foto av sig själv och låter applikationen skanna av den data som finns lagrad i passhandlingen.

på identitetsnivå styrkt identitet. Detta framgår av 26 a och 26 b §§ folkbokföringslagen (1991:481) och av 2 kap. 2 och 3 §§ lagen (2022:1697) om samordningsnummer. Syftet med personlig inställelse i dessa ärenden är en stärkt identitetskontroll för att motverka att felaktiga uppgifter registreras i folkbokföringsverksamheten.[22] Vid en gränskontroll eller inre utlänningskontroll görs granskningen av passhandlingen, av naturliga skäl, i den enskildes personliga närvaro. Även vid en ansökan om pass och nationellt identitetskort krävs personlig inställelse, enligt 6 § passlagen (1978:302) och 3 § förordningen (2005:661) om nationellt identitetskort. Detsamma ska gälla vid ansökan om det statliga identitetskort som föreslagits i promemorian *Ett statligt identitetskort* och som ska ersätta det nationella identitetskortet.[23]

Den enskilde har ofta ett naturligt incitament att medverka till att lämna över handlingar som behövs för att verifiera hans eller hennes identitet. En ansökan kan annars komma att avslås redan på grund av att kravet på styrkt identitet inte är uppfyllt (se MIG 2011:11 avseende uppehållstillstånd och 11 § 1 medborgarskapslagen). Ett annat exempel är att en person riskerar att nekas inresa i Sverige enligt artikel 14.1 i gränskodexen[24] om han eller hon i samband med en gränskontroll inte kan visa upp en giltig passhandling. I vissa situationer kan personen emellertid ha ett intresse av att medvetet undanhålla identitetshandlingar eller helt sakna handlingar, exempelvis vid en inre utlänningskontroll eller vid en ansökan om internationellt skydd.[25] Att det förekommer att identitetshandlingar medvetet undanhålls har konstaterats i tidigare utredningar.[26] Polismyndigheten, Migrationsverket och Skatteverket har därför vissa möjligheter att vidta åtgärder för att få tillgång till en handling. Nedan ges en kort översikt av dessa möjligheter. Lagrumshänvisningar avser bestämmelser i utlänningslagen om inte annat särskilt anges; kursivering avser bestämmelser som inte har trätt i kraft.

[22] *Stärkt system för samordningsnummer*, prop. 2021/22:276 s. 58.
[23] Ju2026/01595, s. 71.
[24] Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016.
[25] Av statistik från Migrationsverket för år 2012 till 2023 framgår att endast cirka 25 procent av de som beviljades uppehållstillstånd som asylsökande hade visat upp en giltig passhandling, se RiR 2024:12, s. 34.
[26] Se exempelvis *Verkställighet vid oklar identitet m.m.*, SOU 2003:25, s. 136 ff.

Tabell 7.2 Åtgärder för att kunna få tillgång till identitetshandlingar

Vid..	… kan följande åtgärder vidtas	… med stöd av
Gränskontroll	Kroppsvisitation, undersökning av bagage, handresgods och handväskor.	9 kap. 2 §
Inre utlänningskontroll	Skyldighet att överlämna pass eller andra handlingar.	9 kap. 9 §
	Kroppsvisitation och undersökning av bagage, om det kan antas att utlänningen har handlingar med sig men på begäran inte överlämnar dessa.	9 kap. 9 a §
	Omhändertagande av pass och andra identitetshandlingar.	9 kap. 4 a §
Uppehållstillstånd	Omhändertagande av pass och andra identitetshandlingar.	9 kap. 4 § första stycket
	Kroppsvisitation och undersökning av bagage, om det kan antas att utlänningen har handlingar med sig men på begäran inte överlämnar dessa.	9 kap. 4 § andra stycket[1]
Ansökan om internationellt skydd	Tillämpning av påskyndat förfarande, bedömning av ansökan som ogrundad.	Artikel 28.6, 39.4 och 42.1 c i screeningförordningen
Inflyttning till Sverige	Skyldighet att på begäran överlämna pass eller andra handlingar.	26 b § folkbokföringslagen
Tilldelning av samordningsnummer	Skyldighet att på begäran överlämna pass eller andra handlingar.	2 kap. 3 § lagen om samordningsnummer

[1] Prop. 2025/26:263, s. 114 f.

Om personen gör motstånd finns stöd i 10 § 4 polislagen (1984:387) för polisman att, i den mån andra medel är otillräckliga och det med hänsyn till omständigheterna är försvarligt, använda våld för att utföra åtgärder i form av bland annat kroppsvisitation. Om personen inte vill gå med på att lämna från sig handlingarna får Migrationsverket, enligt 9 kap. 10 § utlänningslagen[27], begära biträde av Polismyndigheten för att genomföra åtgärden. Tvång kan då användas.

Utöver ovanstående har vi i nationell rätt inte kunnat finna något rättsligt stöd för myndigheter eller privata aktörer att förmå den vars identitet behöver verifieras att överlämna pass eller andra identitetshandlingar för kontroll. Till viss del kan det hänföras till att behov av sådana åtgärder saknas i ärenden där ansökan kan avslås på grund av att identiteten inte är styrkt. Även i sådana ärenden anser vi emeller-

[27] Bestämmelsen ska från och med den 13 juli 2026 ha en ny beteckning, 9 kap. 29 §.

tid att det är av vikt att identitet kan verifieras på ett tillförlitligt sätt, i vart fall för att minska risken för att den enskilde i framtida ärenden uppträder i en annan identitet. Vi kan notera att när det gäller förmåner som handläggs av Försäkringskassan, Pensionsmyndigheten och kommuner saknas bestämmelser som ställer upp ett visst beviskrav angående identiteten eller anger att sökanden ska visa upp en identitetshandling. För privatpersoner som vill använda Försäkringskassans självbetjäningstjänster är det i praktiken fråga om användande av en e-legitimation, ofta BankID. Digitaliseringen har inneburit att majoriteten av alla ansökningar om förmåner hos Försäkringskassan och Pensionsmyndigheten görs med e-legitimation. Dessa myndigheter får därmed tillgång till fysiska identitetshandlingar endast om den enskilde väljer att visa upp eller använda sådana handlingar. I Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* konstaterades att det i socialförsäkringsärenden finns stora risker med att säkerställa att en person som ansöker om förmåner faktiskt är den han eller hon utger sig för att vara, vilket kan leda till felaktiga utbetalningar.[28]

Särskilt om förslag avseende digitala kopior av handlingar

De åtgärder som framgår av tabellen ovan syftar till att den myndighet som ska verifiera identitet ska få tillgång till fysiska identitetshandlingar som personen i fråga kan ha med sig. I betänkandet *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll* konstaterades emellertid att det inte sällan är så att kopior på identitetshandlingar sparas i digitala medier, såsom mobiltelefoner, datorer eller surfplattor. Tillgång till sådan information och en möjlighet att omhänderta och undersöka utrustning som kan innehålla information om identiteten ökar förutsättningarna för att kunna verifiera identiteten. Förslag har därför lämnats på nya bestämmelser i 9 kap. utlänningslagen, som innebär att Polismyndigheten och Migrationsverket under vissa förutsättningar ska få vidta sådana åtgärder.[29]

Enligt förslaget till en ny 9 kap. 19 § utlänningslagen ska Polismyndigheten, vid en inre utlänningskontroll, om det är nödvändigt för att fastställa en utlännings identitet, få besluta om att omhänderta

[28] RiR 2024:12, s. 6.
[29] Prop. 2025/26:263, s. 79 ff.

elektronisk kommunikationsutrustning som denne har i sin besittning, som sannolikt har använts av honom eller henne och som kan antas innehålla information om identiteten. Ett sådant beslut ska enligt 20 § även få fattas av Polismyndigheten och Migrationsverket vid en ansökan om uppehållstillstånd som ges in vid eller efter inresa i landet, under förutsättning att utlänningen inte kan göra sannolikt att den uppgivna identiteten är riktig och att rätten till uppehållstillstånd inte kan bedömas ändå. En polisman ska enligt förslaget till 26 § få kroppsvisitera utlänningen och undersöka utlänningens bagage, handresgods, handväskor och liknande, om det kan antas att han eller hon har med sig sådan utrustning som kan omhändertas. Omhändertagen utrustning ska enligt förslaget till 23 § få undersökas, och de handlingar som påträffas vid undersökningen ska få kopieras. Undersökningen föreslås få omfatta information som lagras både i och utanför det fysiska föremålet, det vill säga även i exempelvis chattapplikationer i en telefon eller i sociala medier som kan nås via telefonen. Någon fast åldersgräns för när dessa åtgärder ska få användas föreslogs inte utan ett barns ålder föreslogs beaktas särskilt vid den proportionalitetsavvägning som ska göras inför beslutet om tvångsåtgärden.

Granskning av handlingar

Som konstaterats inledningsvis behöver en kontroll ofta göras av om en handling är att betrakta som äkta och om den är utfärdad till innehavaren. Det kan ske på olika sätt. För det första kan en okulär jämförelse göras mellan den person som myndigheten eller en privat aktör möter och det fotografi som finns på handlingen. Det är inte fråga om en biometrisk verifiering eftersom ansiktsbilden inte är föremål för en särskild teknisk bearbetning. En sådan okulär jämförelse görs exempelvis vid en gränskontroll, men är även den metod som används av privata aktörer när identiteten kontrolleras av någon anledning, till exempel vid inpassering till en byggnad eller för att säkerställa att den som handlar på Systembolaget har fyllt 20 år. Kontrollen sker då förhållandevis snabbt. Endast en jämförelse av dessa uppgifter kan enligt vår bedömning inte anses ge någon garanti för att innehavaren av handlingen också är den person som myndigheten möter utan innebär betydande tillförlitlighetsbrister; i betänkandet

Om folkbokföring, samordningsnummer och identitetsnummer anförde Skatteverket att det mänskliga ögat sällan kan med fullkomlig säkerhet avgöra att det är samma person på ett foto som den som står framför en.[30] Vi delar den bedömningen.

För det andra kan handlingen granskas genom en kontroll eller närmare granskning av dokumentets fysiska utformning. I samband med en gränskontroll kontrolleras bland annat att samtliga sidor i ett pass ser äkta ut, och genom en passläsare kontrolleras att de alfanumeriska uppgifter som finns lagrade elektroniskt i passet stämmer med den fysiska handlingen. Om passhandlingen av någon anledning kräver ytterligare granskning kan utrustning i form av lupp, UV-lampor och mikroskop användas, och på flygplatser finns tillgång till avancerad utrustning som hanteras av dokumenttekniker. Ett pass som är tekniskt äkta men utfärdat i fel identitet skulle däremot svårligen upptäckas i en gränskontroll.[31]

Migrationsverket skiljer sedan november 2022 mellan tre standardiserade nivåer för undersökning av identitetshandlingar: nivå 0 (dokumentkontroll), nivå 1 (dokumentgranskning) och nivå 2 (äkthetsbedömning). Vid en dokumentkontroll görs en okulär kontroll och handlingen granskas med hjälp av enkel utrustning såsom passläsare, UV-lampa och lupp. Vid anmärkningar eller avvikelser, eller om det finns tips om att något inte står rätt till, görs en mer grundlig dokumentgranskning av certifierade dokumentgranskare vid Migrationsverket eller av id-sambandsmän vid utlandsmyndigheterna. En äkthetsgranskning görs endast vid Migrationsverkets dokumentverifieringsenhet, av experter som genomgått särskild utbildning. Det är få ärenden som lyfts till högre nivåer.[32]

[30] SOU 2021:57, s. 232.
[31] RiR 2024:12, s. 44 och 51.
[32] RiR 2024:12, s. 36 ff.

Tabell 7.3 Översikt av Migrationsverkets dokumentgranskning

Ärenden om internationellt skydd	Tillståndsärenden	Svenskt medborgarskap
Granskning enligt nivå 1 eller 2 utförs på samtliga handlingar som lämnas in av certifierad dokumentgranskare eller id-enhet	Granskning enligt nivå 0, 1 eller 2 utförs på utlandsmyndighet (av lokalanställda, utsända handläggare eller av utsänd id-samordnare)	Granskning enligt nivå 0, 1 eller 2 utförs av handläggare, certifierad dokumentgranskare eller dokument-verifieringsenhet

I ärenden om inflyttning till Sverige och tilldelning av samordningsnummer gör anställda på Statens servicecenter en maskinell kontroll av MRZ-koden (*Machine Readable Zone*) på passet och en kontroll med UV-ljus.[33] Vid ansökan om Schengenvisering ska en kontroll av äktheten och tillförlitligheten i resehandlingar och andra handlingar av betydelse göras. Enligt EU-kommissionens handledning för handläggning av viseringsansökningar är rekommenderad bästa praxis för kontroll av om en resehandling utgör en efterbildning eller förfalskning bland annat att jämföra med ett garanterat äkta exemplar av handlingen, att undersöka handlingen noggrant och att använda utrustning som UV-lampor och förstoringsglas.[34]

Förutom kontroll med hjälp av en elektronisk passläsare är övriga kontrollmetoder delvis beroende av kompetensen hos och bedömningen av den enskilda tjänsteman som utför kontrollen och av tillgången till teknisk utrustning, för att okulärt undersöka en identitetshandling. Som exempel på detta framgår av rapporten *Vem där – fastställande av identitet vid statliga myndigheter* att vid inre utlänningskontroll används generella kunskaper i dokumentgranskning som har getts vid polisutbildningen, och flera beslutsfattare och dokumenttekniker som Riksrevisionen då intervjuade beskrev medarbetarnas kunskap som låg i förhållande till uppgiftens komplexitet, med följden att falska handlingar riskerar att missas.[35]

Som konstaterades i betänkandet *Ett säkert statligt ID-kort – med e-legitimation* är det den som identitetshandlingen visas upp för som själv ansvarar för att bedöma om en viss handling är äkta och giltig.

[33] RiR 2024:12, s. 64.
[34] Kommissionens beslut K(2010)1620 av den 19 mars 2010.
[35] RiR 2024:12, s. 49.

Kontroll av om en handling är äkta kan i huvudsak endast göras genom att de säkerhetsdetaljer som finns på den granskas manuellt.[36] I vilken utsträckning eller hur detta sker i andra situationer än de som beskrivits ovan är enligt vår bedömning inte möjligt att redogöra för i detta sammanhang.

Biometriska kontroller mot handlingar

En mer tillförlitlig metod för att bekräfta att en handling är utfärdad till den person som myndigheten möter är att använda biometriska uppgifter. Genom att en kontroll görs av de biometriska uppgifter som kan tas fram ur de biometriska underlag som finns lagrade i handlingen görs indirekt en kontroll av de uppgifter som personen lämnat till svenska myndigheter om sin identitet i ett tidigare ärende. Detta har lyfts i tidigare utredningar, bland annat av Utredningen om folkbokföring och samordningsnummer, som bedömde att en kontroll av biometriska uppgifter i samband med en anmälan om flytt till Sverige och vid tilldelning av samordningsnummer kan utgöra ett effektivt verktyg för Skatteverket i dess arbete för att minska felen i folkbokföringsdatabasen.[37] Nya bestämmelser som möjliggör detta infördes därför i folkbokföringslagen och lagen om samordningsnummer. Sedan Skatteverket gavs en möjlighet att jämföra biometriska uppgifter vid en identitetskontroll har myndigheten emellertid endast genomfört sådana kontroller av ansiktsbilder. Myndigheten har alltså inte genomfört några sådana kontroller av fingeravtryck. I syfte att främja användningen av biometriska uppgifter har förslag lämnats om att Skatteverkets folkbokföringsverksamhet ska få möjlighet att ta fram biometriska uppgifter även ur en ansiktsbild som är synlig på en identitetshandling eller ett uppehållstillståndskort, för att kontrollera biometriska uppgifter vid en identitetskontroll.[38]

Polismyndigheten, Migrationsverket och Skatteverket har, beroende på ärendeslag, vissa möjligheter att ta upp biometriska underlag för att, med de biometriska uppgifter som kan tas fram ur underlagen, göra en en-till-en-jämförelse mot uppgifter som finns lagrade i en

[36] SOU 2019:14, s. 354.
[37] SOU 2021:57, s. 230.
[38] Jfr *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 385 och prop. 2025/26:261, s. 52 f.

handling som den enskilde har åberopat till stöd för sin identitet. Stöd för detta finns bland annat i EU-förordningar på utlänningsrättens område och i 9 kap. utlänningslagen, där särskilt följande kan nämnas. Vid gränskontroller kan, enligt artikel 8.3 i gränskodexen, biometriska underlag i resehandlingar kontrolleras, dock endast för tredjelandsmedborgare. För personer som ansöker om internationellt skydd ska kontrollen, enligt artikel 14.6 i screeningförordningen, bland annat innefatta en verifiering av minst en av de biometriska uppgifter som finns lagrade i en identitetshandling, resehandling eller annan handling. Enligt 9 kap. 8 b § utlänningslagen kan handlingar som har utfärdats av Migrationsverket, bland annat uppehållstillståndskort, kontrolleras både vid gränskontroller och i samband med en inre utlänningskontroll, oavsett om den avser en tredjelandsmedborgare eller EES-medborgare. Vid en ansökan om uppehållstillstånd som görs innan inresa eller visering saknas däremot bestämmelser som ger Migrationsverket eller utlands–myndigheterna rätt att ta upp biometriska underlag av sökanden för att kunna kontrollera de biometriska uppgifter som kan tas fram ur dessa mot en åberopad handling, utan dokumentkontrollen består i första hand av en granskning av dokumentets utformning. I detta sammanhang kan vi notera att det i betänkandet *Registrering av EES-medborgare* föreslogs att ett särskilt registreringsförfarande för EES-medborgare ska återinföras och att en ny bestämmelse ska införas i 9 kap. 8 k § utlänningslagen, som innebär att en EES-medborgare ska vara skyldig att, i ett ärende om registrering av uppehållsrätt, låta Migrationsverket fotografera honom eller henne och ta hans eller hennes fingeravtryck; en jämförelse ska i samband med detta få göras mot biometriska uppgifter som kan tas fram ur ett pass eller ett identitetskort som visas upp och som har ett lagringsmedium där fotografi eller fingeravtryck är sparade eller har ett synligt fotografi.[39]

Vid ansökan om pass och nationellt identitetskort saknas i nuläget möjlighet att använda de biometriska uppgifter som tas fram vid ansökan för att kontrollera sådana uppgifter som kan tas fram ur biometriska underlag i en handling som sökanden använt för att styrka sin identitet. I promemorian *Ett statligt identitetskort* föreslogs dock en ny lag om statligt identitetskort, som bland annat innebär att en sådan kontroll ska kunna göras vid ansökan om det

[39] SOU 2026:9, s. 39 och 194 ff.

statliga identitetskort som föreslogs, samt vid ansökan om pass.[40] Vid utfärdande av en sådan statlig e-legitimation som föreslagits i propositionen *En statlig e-legitimation* ska en motsvarande kontroll kunna göras.[41]

Nedan ges en översikt av gällande, beslutat och föreslaget rättsligt stöd för att kontrollera biometriska underlag i identitetshandlingar som finns i relevanta ärendeslag. Lagrumshänvisningar avser bestämmelser i utlänningslagen om inte annat särskilt anges. Kursiverade bestämmelser är förslag som har lämnats.

Tabell 7.4 Möjlighet att kontrollera biometriska underlag i identitetshandlingar

Vid …	… kan biometri kontrolleras i	… med stöd av
Gränskontroll	Uppehållstillståndskort, uppehållskort, permanent uppehållskort, bevis om uppehållsstatus eller bevis för gränsarbetare	9 kap. 8 b §
	Resehandlingar	9 kap. 8 c §
	Passhandling	5 a § passlagen
	Schengenvisering	9 kap. 8 d §
Inre utlänningskontroll	Uppehållstillståndskort, uppehållskort, permanent uppehållskort, bevis om uppehållsstatus eller bevis för gränsarbetare	9 kap. 8 b §
Ansökan om internationellt skydd	Identitetshandling, resehandling eller annan handling	9 kap. 8 § 2 samt artikel 9.1 b och 14.6 i screeningförordningen
Inflyttning till Sverige	Pass, identitetskort, uppehållstillståndskort och annan motsvarande handling	26 c § folkbokföringslagen[1]
Tilldelning av samordningsnummer	Pass, identitetskort, uppehållstillståndskort och annan motsvarande handling	2 kap. 4 § lagen om samordningsnummer
Naturalisation	Uppehållstillståndskort	*13 f § medborgarskapslagen*[2]
Ansökan om statligt id-kort	Handlingar som används för att styrka identitet och innehåller ansiktsbild eller fingeravtryck samt ett statligt id-kort som lämnas ut.	*3 kap. 5 § och 4 kap. 2 § lag om statligt identitetskort*[3]

[40] Ju 2026/01595, s. 191 och 221 f.
[41] Prop. 2025/26:250, s. 60 f.

Vid …	… kan biometri kontrolleras i	… med stöd av
Ansökan om pass	Handlingar som används för att styrka identitet och innehåller ansiktsbild eller fingeravtryck samt ett pass som lämnas ut.	*6 a § och 11 c § passlagen*[4]
Utfärdande av uppehållstillståndskort	Uppehållstillståndskort, permanent uppehållskort, bevis om uppehållsstatus eller bevis för gränsarbetare	*9 kap. 8 k §*[5]
Registrering av uppehållsrätt	Pass och identitetskort	*9 kap. 8 k §*[6]

[1] Enligt förslag i prop. 2025/26:261 ska den nuvarande bestämmelsen flyttas till en ny bestämmelse, 26 d §. Detsamma gäller bestämmelsen i 2 kap. 4 § lagen om samordningsnummer, som föreslås flyttas till en ny bestämmelse, 2 kap. 4 a §.
[2] Prop. 2025/26:263, s. 155 ff.
[3] Promemorian Ett statligt identitetskort, Ju2026/01595, s. 191 f.
[4] Ju2026/01595, s. 221.
[5] Prop. 2025/26:263, s. 133 ff.
[6] SOU 2026:9, s. 194.
[7] Åtgärder mot mervärdesskattebedrägerier, prop. 2025/26:128, s. 39 f.

Det finns alltså flera gällande och föreslagna möjligheter för Polismyndigheten, Migrationsverket och Skatteverket att med hjälp av biometriska uppgifter koppla identitetshandlingar – och andra handlingar som innehåller identitetsuppgifter – till den person som myndigheten möter och de identitetsuppgifter som han eller hon gör gällande. Vid en ansökan om förmåner som hanteras av Försäkringskassan, Pensionsmyndigheten och kommunerna saknas däremot bestämmelser som ger myndigheterna möjlighet att koppla en eventuell identitetshandling till den sökande genom användning av biometriska uppgifter. Något rättsligt stöd för andra myndigheter eller privata aktörer att använda biometriska uppgifter för att kontrollera handlingar av olika slag har vi inte heller kunnat finna. Det kan i detta sammanhang noteras att i betänkandet från 2017 års ID-kortsutredning gjordes bedömningen att det inte bör införas någon skyldighet för den som innehar en handling som innehåller biometriska uppgifter att i andra sammanhang än vid gränskontroller och vid ansökan om ett statligt id-kort eller pass lämna sådana uppgifter för kontroll av

om dessa motsvarar dem som finns lagrade på handlingen.[42] Vi återkommer till detta i avsnitt 10.5.

7.4.3 Verifiering mot uppgifter i ett register

I många fall kan en tillförlitlig verifiering av identiteten ske genom att den enskilde lämnar in en godtagbar identitetshandling som på ett säkert sätt kan kopplas till honom eller henne genom en biometrisk jämförelse mot biometriska underlag som är lagrade i handlingen. Det kan då framstå som onödigt från processekonomisk synvinkel att också genomföra sökningar i olika register i sådant syfte, när sådan möjlighet finns. Beroende på ärendeslaget kan det dock finnas en skyldighet för myndigheten i fråga att söka i tillgängliga informationssystem för att biometriskt verifiera identitet. Exempelvis ska Polismyndigheten, enligt artikel 8.2 a i gränskodexen, verifiera identitet vid en gränskontroll genom en sökning i bland annat SIS. Sökningar i EU-gemensamma informationssystem för att verifiera identitet är också av vikt för att främja de mål som EU-förordningar på utlänningsrättens område eftersträvar. Av skäl 15 till in- och utreseförordningen framgår exempelvis att målet för in- och utresesystemet är att förbättra förvaltningen av de yttre gränserna, förhindra irreguljär invandring och underlätta hanteringen av migrationsströmmar, genom att i tillämpliga fall bidra till identifiering av personer som inte uppfyller, eller inte längre uppfyller, villkoren för längden på den tillåtna vistelsen på medlemsstaternas territorium. En sökning i register som innehåller identitetsuppgifter och/eller biometriska uppgifter är dessutom av vikt i de fall den identitet som görs gällande är oklar, exempelvis på grund av att en asylsökande saknar hemlandspass. Sökningar kan även göras i andra syften än att verifiera identitet, till exempel för att avgöra om en person utgör ett hot mot den allmänna ordningen eller vilken medlemsstat som är ansvarig för att pröva en asylansökan. Dessa situationer behandlas dock inte i detta sammanhang.

De sökningar som kan genomföras i relevanta och tillgängliga system för att verifiera identitet kan göras antingen med hjälp av alfanumeriska uppgifter – i första hand identitetsuppgifter – eller biometriska uppgifter. Vid en sökning mot en hel databas med bio-

[42] SOU 2019:14, s. 311.

metriska uppgifter är det emellertid fråga om *identifiering* av en person, vilket vi har redogjort närmare för i avsnitt 7.3. Inte bara alfanumeriska uppgifter om identitet kan ligga till grund för sökningen för att lokalisera en träff som kan användas för verifiering. Exempelvis kan, enligt artikel 18 och 22g i VIS-förordningen, en sökning göras med hjälp av numret på en visering eller ett uppehållstillstånd.

Sökning med alfanumeriska uppgifter

Med utgångspunkt i det identitetsbegrepp som vi definierat i avsnitt 3.2 – vilket omfattar namn, födelsetid och medborgarskap – är det inte osannolikt att en sökning i olika register enbart med dessa uppgifter resulterar i flera träffar. Även om det endast blir en enda träff innebär det inte med säkerhet att träffen avser samma individ som myndigheten möter, och det ger inte i sig någon ytterligare information om tillförlitligheten i de uppgifter som personen har lämnat om sin identitet. Syftet med en alfanumerisk sökning är som vi ser det i stället i första hand att få fram en träff, mot vilken biometriska uppgifter eller andra uppgifter kan jämföras, genom en en-till-en-jämförelse. Andra uppgifter som kan användas för jämförelsen kan till exempel vara en resehandlings typ och nummer, ansiktsbilder som inte utgör biometriska uppgifter eller andra uppgifter som kan ha kommit fram i ärendet och som kan kontrolleras mot dem som finns lagrade i databasen för den träff som sökningen resulterade i. Sådana uppgifter kan ha kommit fram under en muntlig intervju, vid en språkanalys eller vid förfrågningar till svenska beskickningar utomlands som har möjlighet att vidta utredningsåtgärder för att få fram uppgifter om identitet från exempelvis folkbokföringsregister i den enskildes hemland.

Det finns ett relativt brett stöd i EU-förordningar på utlänningsrättens område för att söka i olika gemensamma informationssystem för att verifiera identitet. Förordningarna innehåller dock vissa begränsningar i fråga om personkretsen. Vid inre utlänningskontroller och i ärenden om uppehållstillstånd är möjligheten att söka i SIS med stöd av artikel 34.1 i gränsförordningen begränsad till tredjelandsmedborgare. Vid gränskontroller och i ärenden om naturalisation kan en sökning göras även avseende EES-medborgare,

då enligt artikel 8.2 a i gränskodexen respektive artikel 34.2 i gränsförordningen. In- och utreseförordningen är enligt artikel 23.2 och 26 begränsad till tredjelandsmedborgare och möjligheten att söka i EU:s centrala databas för identitetsuppgifter, CIR, enligt artikel 14.2 i screeningförordning, är begränsad till personer som ansöker om internationellt skydd, i situationer då identiteten inte redan har verifierats enligt artikel 8 i gränskodexen. VIS-förordningen, som i artikel 18, 19, 22g och 22h innehåller stöd för att söka med alfanumeriska uppgifter vid en inre utlänningskontroll eller gränskontroll, är ännu mer begränsad i dessa ärenden, då den endast omfattar de tredjelandsmedborgare som innehar en visering eller ett uppehållstillstånd. När det gäller sökningar med alfanumeriska uppgifter i nationella register som den centrala utlänningsdatabasen och i folkbokföringsverksamheten finns det däremot inte några begränsningar i personkretsen.

Nedan ges en översikt av när sökningar med alfanumeriska uppgifter kan göras i olika ärendeslag. När det gäller skyldigheten för Migrationsverket att lämna uppgifter till Skatteverket enligt 7 kap. 15 b § utlänningsförordningen i ärenden om inflyttning till Sverige och tilldelning av samordningsordningsnummer ska noteras att det sker genom utlämnande på medium för automatiserad behandling. Det är alltså inte fråga om att Skatteverket genom direktåtkomst kan göra sökningar i den centrala utlänningsdatabasen.[43]

[43] SOU 2025:75, s. 502.

Tabell 7.5 Sökningar med alfanumeriska uppgifter

Vid …	… kan uppgifter hämtas från	… med stöd av
Gränskontroll	SIS	Artikel 33.1 i gränsförordningen och 11 § 1 förordningen (2021:1188)
	In- och utresesystemet	Artikel 23.2 i in- och utreseförordningen
	VIS	Artikel 18 och 22g i VIS-förordningen
	CIR (asylsökande)	Artikel 14.2 i screeningförordningen och artikel 20a i IOF
	Centrala utlännings-databasen, CUD	9 § utlänningsdataförordningen och 11 § 2 och 19 § utlänningsdatalagen
	Navet	14 § folkbokföringsdatalagen (2026:126)
Inre utlänningskontroll	SIS	Artikel 33.1 i gränsförordningen och 11 § 1 förordningen (2021:1188)
	In- och utresesystemet	Artikel 26.1 i in- och utreseförordningen
	VIS	Artikel 19 och 22.h i VIS-förordningen
	CUD och Navet	Samma som vid gränskontroller
Uppehållstillstånd	SIS	Artikel 33.1 i gränsförordningen och 11 § 4 förordningen (2021:1188)
	In- och utresesystemet (tillståndsärenden)	Artikel 3.1.4 b, 9.2 och 26.1 i in- och utreseförordningen
	CIR (skyddsbehov)	Artikel 14.2 i screeningförordningen och artikel 20a i IOF
	CUD	11 § 1 utlänningsdatalagen
	Navet	14 § folkbokföringsdatalagen
Medborgarskap	SIS (naturalisation)	Artikel 34.2 i gränsförordningen och 11 § 7 förordningen (2021:1188)
	CUD	11 § 1 utlänningsdatalagen
Viseringar	VIS (även den europeiska sökportalen ESP)	Artikel 15.2 b (och 9a) i VIS-förordningen
	SIS	Artikel 33.1 och 34.1 d och f i gränsförordningen samt 11 § 4 och 6 § förordningen (2021:1188)
	CUD och Navet	Samma som i ärenden om uppehållstillstånd
Inflyttning till Sverige	CUD	10 kap. 27 § OSL och 7 kap. 15 b § utlänningsförordningen
Tilldelning av samordningsnummer	CUD	10 kap. 27 § OSL och 7 kap. 15 b § utlänningsförordningen
Övriga ärenden	Navet	14 § folkbokföringsdatalagen

För privata aktörer saknas rättsliga möjligheter att söka i något av de register som anges i tabellen ovan. I stället finns möjlighet att i egenskap av kund göra sökningar i bland annat Statens personadressregister, SPAR, som är ett offentligt register som omfattar alla personer som är folkbokförda i Sverige och som har tilldelats samordningsnummer på de två högsta identitetsnivåerna; styrkt och sannolik identitetsnivå. SPAR får även innehålla uppgifter om personer som varit folkbokförda. Registret förs av Skatteverket. Många banker samt försäkrings- och kreditupplysningsföretag uppdaterar sina register via SPAR.

En bedömning av om det kan bekräftas att en påstådd identitet är riktig genom en jämförelse med uppgifter som hämtats ur ett register, med hjälp av en sökning med alfanumeriska uppgifter, beror som vi ser det på omständigheterna i det enskilda fallet – i stor utsträckning på om det finns andra sidouppgifter som kan jämföras med de som lämnats av den enskilde eller som på andra sätt har kommit fram i ärendet. Som vi anfört ovan kan en träff utifrån en sökning med alfanumeriska identitetsuppgifter i sig inte anses bekräfta en påstådd identitet. I ärenden om förmåner som handläggs av Försäkringskassan hämtar myndigheten in uppgifter automatiskt från folkbokföringsverksamheten via Navet. Sökningen i Navet görs endast med alfanumeriska uppgifter om identitet som sökanden lämnat.[44] Det finns därför en risk för att de uppgifter som hämtas in inte avser sökanden, i vart fall inte utan att andra uppgifter som lämnats och som finns knutna till träffen samtidigt jämförs, exempelvis om adress och civilstånd. Även i sådana fall kan myndigheten, enligt vår mening, svårligen anses ha fått svar på frågan *Är sökanden den som han eller hon påstår sig vara?*

Jämförelse med biometriska uppgifter i ett register

Om sökningen med alfanumeriska uppgifter i ett register resulterar i en möjlig träff kan en biometrisk verifiering göras genom att de biometriska uppgifter som tagits fram ur fingeravtryck eller ansiktsbilder som har tagits upp av den enskilde jämförs med de som är lagrade i registret; detta utgör det första steget i verifieringen på det sätt vi beskrivit i avsnitt 7.2.1. Om den alfanumeriska sökningen har gett

[44] RiR 2024:12, s. 68.

flera träffar uppkommer frågan om en-till-en-jämförelser bör göras mot var och en av träffarna eller om en identifiering med biometriska uppgifter i stället bör genomföras. Med hänsyn till vad vi anfört i avsnitt 7.4.1 bör utgångspunkten vara att identifiering genom en sökning med biometriska uppgifter mot hela databasen undviks, innan en biometrisk verifiering mot ett mer begränsat träffresultat har gjorts. Myndigheten kan även vidta olika utredningsåtgärder i syfte att få fram ytterligare uppgifter om den enskilde som, genom en alfanumerisk sökning, kan ge en enda träff. Vilken metod som bör användas i ett enskilt fall är inte närmare reglerat och vi avser inte heller att närmare ta ställning till hur myndigheter som har att verifiera identitet generellt sett bör agera.

Stöd för att använda biometrisk verifiering mot ett register finns i flera EU-gemensamma förordningar på utlänningsrättens område. I samband med inre utlänningskontroller och gränskontroller kan en verifiering göras mot biometriska uppgifter som är lagrade i in- och utresesystemet, SIS och VIS, med stöd av artikel 26.1 och 23.2 i in- och utreseförordningen, artikel 33.1 i gränsförordningen samt artikel 18, 19, 22g och 22h i VIS-förordningen. Det är i första hand tredjelandsmedborgare som omfattas. Sökningar i VIS avser dessutom endast personer som innehar en visering eller ett uppehållstillstånd. För utlänningar som genomgår screening kan biometrisk verifiering göras med stöd av artikel 14.2 i screeningförordningen, i fall då identiteten inte redan har verifierats enligt artikel 8 i gränskodexen. I tillståndsärenden kan biometrisk verifiering göras av Migrationsverket enligt artikel 26.1 i in- och utreseförordningen, dock endast i ärenden där sökanden befinner sig i Sverige, vilket betydligt begränsar tillämpningsområdet i praktiken. Förutom screeningförordningen – som hänvisar till Eurodacförordningen – innehåller förordningarna inte något uttryckligt stöd för myndigheter att ta upp de biometriska underlag som används för jämförelsen, utan de reglerar åtkomsten till, och möjligheten att söka i, systemen. Kompletterande bestämmelser finns därför i 9 kap. utlänningslagen. Personkretsen som omfattas av dessa bestämmelser är i viss mån begränsad, genom att gällande och föreslagna bestämmelser endast ger stöd för att ta fingeravtryck om utlänningen har fyllt sex år eller, när det gäller verifiering enligt artikel 26 i in- och utreseförordningen, tolv år (se 9 kap. 8 h § utlänningslagen). När det gäller biometriska underlag som finns i Migrationsverkets register över fingeravtryck och fotografier är de be-

gränsade på så sätt att de endast omfattar personer som tillhör den personkrets vars biometriska underlag kan, och ska kunna, tas upp med stöd av bestämmelserna i 9 kap. utlänningslagen. I regeringens proposition *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* föreslås att Migrationsverket ska kunna jämföra biometriska uppgifter som tas fram i asylärenden mot sådana uppgifter som, enligt de förslag som lämnas i andra delar av betänkandet, kommer att lagras hos Skatteverket. En motsvarande möjlighet för Skatteverket att använda Migrationsverkets register över fingeravtryck och ansiktsbilder för att biometriskt verifiera identitet i ärenden om inflyttning till Sverige och tilldelning av samordningsnummer föreslås samtidigt.[45]

I samband med ansökan om och utfärdande av ett svenskt hemlandspass och ett nationellt identitetskort saknas i nuläget möjlighet att använda register som förs av Polismyndigheten eller andra myndigheter för att biometriskt kontrollera sökandens identitet. I promemorian *Ett statligt identitetskort* lämnas emellertid förslag om ett pass- och identitetskortsregister som ska få innehålla biometriska uppgifter som har tagits fram ur den ansiktsbild som tas av sökanden och att ansiktsbilden ska få användas för sökning i registret i syfte att kontrollera sökandens identitet. Vidare föreslås att den utfärdande myndigheten ska få göra en biometrisk kontroll av den ansiktsbild som tas av sökanden mot pass- och identitetskortsregistret.[46] När det gäller uppehållstillståndskort utfärdas dessa i den identitet som Migrationsverket har etablerat för den enskilde, efter utredning av identiteten inom ramen för ett ärende om uppehållstillstånd. Vilka möjligheter Migrationsverket har – och genom lagda förslag kommer att ha – att verifiera sökandens identitet biometriskt i ett ärende om uppehållstillstånd beror på grunden för tillståndet. I regeringens proposition *Stärkt återvändandeverksamhet* föreslås att en biometrisk kontroll ska få göras mot Migrationsverkets register över fingeravtryck och ansiktsbilder för att kontrollera sökandens identitet när bland annat ett uppehållstillståndskort ska lämnas ut; en kontroll ska dock i första hand göras mot en tidigare utfärdad handling.[47]

Nedan ges en översikt av när biometrisk verifiering kan göras i olika ärendeslag. Lagrumshänvisningar avser bestämmelser i utlänningslagen om inte annat anges särskilt. Föreslagna bestämmelser

[45] Prop. 2025/26:261, s. 80 f.
[46] Ju2026/01595, s. 208 ff.
[47] Prop. 2025/26:263, s. 133 ff.

är kursiverade. Med Migrationsverkets register avses de register som myndigheten för enligt 15 § utlänningsdatalagen.

Tabell 7.6 Stöd för att använda biometrisk verifiering

Vid …	… kan biometriska underlag tas upp enligt	… för verifiering mot
Gränskontroll	9 kap. 8 § 1	SIS
	9 kap. 8 d §	VIS
	Artikel 6.1 f i gränskodexen	In- och utresesystemet
	9 kap. 8 § 2 och artikel 9.2 b i screeningförordningen	CIR (personer som ansöker om internationellt skydd)
Inre utlänningskontroll	9 kap. 8 f §	SIS
	9 kap. 8 h §	In- och utresesystemet
	9 kap. 8 h §	VIS
	9 kap. 8 § 4	Migrationsverkets register
Uppehållstillstånd	9 kap. 8 a § (samtliga)	In- och utresesystemet
	9 kap. 8 § 2 och 9 kap. 8 a §	SIS
	9 kap. 8 § 1 och 2 (skyddsbehov)	CIR och Migrationsverkets register
		Migrationsverkets register
	9 kap. 8 a § (samtliga)	Folkbokföringsverksamheten[1]
Av- och utvisning	9 kap. 8 § 5	Migrationsverkets register
Schengenvisering	Artikel 13 i viseringskodexen	VIS
Nationell visering	9 kap. 8 j §[2]	VIS
Naturalisation	*13 f § medborgarskapslagen*[3]	Migrationsverkets register
Inflyttning till Sverige	*26 c § första stycket folkbokföringslagen*[4]	Migrationsverkets register och folkbokföringsverksamheten[5]
Tilldelning av samordningsnummer	*2 kap. 4 § lagen om samordningsnummer*[6]	Migrationsverkets register och folkbokföringsverksamheten[7]
Ansökan om pass	*6 a § och 11 c § passlagen*[8]	Pass- och identitetskortsregistret
Ansökan om statligt identitetskort	*3 kap. 5 § och 4 kap. 2 § lag om statligt identitetskort*[9]	Pass- och identitetskortsregistret
Ansökan om uppehållstillståndskort	*9 kap. 8 k §*[10]	Migrationsverkets register

[1] Jämförelsen kan göras med stöd av förslag till en ny punkt 14 i 15 § utlänningsdatalagen, se prop. 2025/26:261, s. 110.

[2] Prop. 2024/25:176, s. 55.

[3] Prop. 2025/26:263, s. 155 ff.

[4] Prop. 2025/26:261, s. 102 ff.

[5] Jämförelsen kan göras med stöd av förslag till nya bestämmelser i 26 d och e §§ folkbokföringslagen, se prop. 2025/26:261, s. 103 f.

[6] Prop. 2025/26:261, s. 113.

[7] Jämförelsen kan göras med stöd av förslag till nya bestämmelser i 2 kap. 4 a och b §§ lagen om samordningsnummer, se prop. 2025/26:261, s. 114 f.

[8] Ju2026/01595, s. 221.

[9] Ju2026/01595, s. 191 f.

[10] Prop. 2025/26:263, s. 133 ff.

Om en-till-en-jämförelse mellan de biometriska uppgifter som finns i aktuellt register och de som tagits fram ur de biometriska underlag som tagits upp av den enskilde i ärendet visar att de matchar, och även de uppgifter om identitet som är kopplade till träffen matchar den påstådda identiteten har myndigheten fått bekräftat att den person som den möter också är den som han eller hon utger sig för att vara. De uppgifter som lämnats om identiteten får därmed anses tillförlitliga och kan läggas till grund för eventuell registrering i den kontrollerande myndighetens egna, eller andra, register, eller för utfärdande av en viss typ av handling.

8 Registrering av uppgifter i vissa register

8.1 Inledning

För att myndigheter och andra aktörer ska kunna verifiera identitet för en person som de kommer i kontakt med förutsätts att det finns ett underlag att jämföra den påstådda identiteten och de biometriska uppgifter som tagits fram mot (jfr avsnitt 7.4.1).

I kapitel 7 har vi beskrivit hur Polismyndigheten, Migrationsverket och Skatteverket genom olika utredningsåtgärder kan verifiera identitet för personer som vistas eller vill vistas i Sverige, exempelvis i samband med en ansökan om uppehållstillstånd eller en inre utlänningskontroll. De alfanumeriska uppgifter om identiteten som myndigheten då har fått fram, samt eventuella biometriska underlag som har tagits upp från personen och biometriska uppgifter som tagits fram ur dessa, kan behöva sparas i myndighetens egna och gemensamma system. Vilka uppgifter som kan registreras och utifrån vilket underlag varierar beroende på ärendeslaget.

De uppgifter som registreras kommer ofta att ligga till grund för senare verifiering av identitet i olika sammanhang eller för en registrering i andra myndigheters system; till exempel ligger Migrationsverkets bedömning av identiteten som utgångspunkt till grund för de uppgifter om identitet som Skatteverket registrerar i folkbokföringsverksamheten för personer som beviljats uppehållstillstånd i Sverige.[1] Biometriska uppgifter som registrerats av en myndighet kan också användas för att identifiera en person, vilket motverkar att någon uppträder i multipla identiteter. I detta kapitel redogör vi för när alfanumeriska uppgifter och biometriska underlag kan registreras i

[1] Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter*, RiR 2024:12, s. 59 f.

de olika ärendeslag som Polismyndigheten, Migrationsverket och Skatteverket ansvarar för som behandlats i kapitel 6. Identiteten behöver också utredas vid en ansökan om ett svenskt pass eller ett nationellt identitetskort, och såväl uppgifter om identiteten som biometriska underlag registreras i den fysiska handling som utfärdas av Polismyndigheten. En betydande del av de personer som vistas i Sverige och har kontakt med myndigheter och andra aktörer i samhället använder sådana handlingar för att i olika sammanhang visa vem han eller hon är. Det är därför av intresse för våra fortsatta överväganden att redogöra även för hur identitetsuppgifter samt biometriska underlag och biometriska uppgifter registreras i dessa ärenden.

I registerförfattningar anges ofta vilka uppgifter som får *behandlas* i registret, se exempelvis 2 § utlänningsdatalagen (2016:27). Detta uttryck omfattar att uppgifterna får *lagras* i registret. I förarbetena till utlänningsdatalagen uttalas att ”Migrationsverket *registrerar* och lagrar fotografier i den centrala utlänningsdatabasen”.[2] Det kan hävdas att lagring har en närmare anknytning till det rent tekniska förfarandet, exempelvis att lagra uppgifterna i en databas eller i en identitetshandling, medan registrering, som vi ser det, ger uttryck för myndighetens åtgärder ur en rättslig synvinkel, vilket är det vi fokuserar på i detta kapitel. Uttrycken får dock i allt väsentligt anses synonyma. Båda uttrycken kan därför komma att användas i detta, och senare, kapitel.

8.2 Allmänt om registrering av uppgifter

De identitetsuppgifter och andra uppgifter som är knutna till en viss person, däribland biometriska underlag och biometriska uppgifter, och som har kommit fram i ett ärende, kan som utgångspunkt behöva registreras vid handläggningen av samtliga ärenden där en grundidentitet kan behöva etableras, det vill säga när det kan konstateras att personen sedan tidigare inte är känd av svenska myndigheter med den identitet som han eller hon har uppgett. Sådana uppgifter kan också behöva registreras när det finns anledning att ändra befintliga uppgifter. Också i sistnämnda fall är det enligt vår mening fråga om att registrera uppgifter; Högsta förvaltningsdomstolen uttalade i rättsfallet HFD 2019 ref. 9, som avsåg ändring av uppgifter om identitet i folkbokföringsdatabasen, att ”det inte klart framgår att de uppgifter som

[2] *Utlänningsdatalag*, prop. 2015/16:65, s. 72

[klaganden] nu önskar *få registrerade* (vår kursivering) är riktiga". Ett exempel på när befintliga uppgifter kan behöva ändras är om en utlänning, som utan att ha gjort identiteten sannolik beviljats tidsbegränsat uppehållstillstånd i egenskap av skyddsbehövande, lämnar in ett hemlandspass till Migrationsverket i samband med en ansökan om att förlänga uppehållstillståndet eller i ett ärende om medborgarskap genom naturalisation. Om de identitetsuppgifter som framgår av passhandlingen skiljer sig från de som utlänningen lämnat i det tidigare ärendet, och bedöms som mer tillförlitliga, kan uppgifterna behöva uppdateras, genom att de nya uppgifterna registreras i den centrala utlänningsdatabasen.

8.2.1 Behovet varierar utifrån ärendeslaget

I praktiken varierar behovet av att faktiskt registrera uppgifter utifrån vilken typ av ärende det är fråga om i ett enskilt fall. I de ärenden där den kontrollerande myndigheten fattar ett beslut efter en ansökan eller anmälan behöver nya uppgifter om sökanden ofta registreras, i vart fall om det är en förstagångsansökan. Det kan röra sig om folkbokföring vid födelse i Sverige, tilldelning av samordningsnummer, visering eller uppehållstillstånd innan eller i samband med inresa till Sverige. I dessa ärenden har personen ofta inte haft kontakt med svenska myndigheter tidigare och uppgifterna om identiteten behöver då registreras, liksom biometriska underlag och biometriska uppgifter, om det finns stöd för det i det aktuella ärendeslaget. Vid ansökningar om internationellt skydd som görs i samband med inresa behöver en ny identitet i stort sett alltid registreras hos Migrationsverket, men vid en ansökan om förlängt uppehållstillstånd behöver några nya uppgifter om identiteten sällan registreras, trots att Migrationsverket fattar ett beslut i ärendet. Behovet att registrera uppgifter korrelerar alltså inte strikt med att myndigheten i fråga fattar ett beslut.

I andra ärendeslag än de ovan nämnda är verifiering av en redan etablerad identitet i stället i fokus. Vid en anmälan om inflyttning från en tredjelandsmedborgare förutsätts att han eller hon har rätt att vistas i landet med stöd av ett uppehållstillstånd, vilket innebär att personen tidigare har haft kontakt med Migrationsverket i det ärendet. Detsamma gäller i ärenden om medborgarskap genom naturalisation, där det som utgångspunkt krävs att sökanden både har hem-

vist i Sverige sedan viss tid och ett uppehållstillstånd, vilket innebär att en identitet redan finns registrerad hos Migrationsverket, och även hos Skatteverket. Vid gränskontroller kan det antas att det endast i fåtal fall är aktuellt för Polismyndigheten att registrera nya uppgifter om identitet för den som kontrolleras. I och med Schengensamarbetet är myndigheten bara ansvarig för att verifiera identitet på personer som reser direkt till Sverige från tredje land och i många fall har personen därför redan haft kontakt med Migrationsverket eller en utlandsmyndighet, som antingen utfärdat en visering för inresa eller beviljat ett uppehållstillstånd. Om personen reser in från ett annat land i Schengenområdet sker inte heller någon gränskontroll vid inresa i Sverige, vilket framgår direkt av artikel 1 andra stycket i gränskodexen[3]. I fall när tredjelandsmedborgare ansöker om internationellt skydd i samband med en gränskontroll bör Polismyndigheten i initialskedet vidta vissa utredningsåtgärder, som att ta upp biometriska underlag för att knyta en identitet till dessa, men har därefter, i enlighet med 6 kap. 14 § utlänningsförordningen (2006:97), att lämna över uppgifterna och ärendet till Migrationsverket, som registrerar uppgifterna inom ramen för ärendet om uppehållstillstånd. Det kan i detta sammanhang framhållas att den omständigheten att en personakt, i enlighet med artikel 6 a i gränskodexen och artikel 14 i in- och utreseförordningen[4], ska skapas för olika kategorier av tredjelandsmedborgare i samband med en gränskontroll inte innebär att identitetsuppgifterna samtidigt ska registreras i nationella register.

Vid inre utlänningskontroller är det enligt vår bedömning endast i ett begränsat antal fall som Polismyndigheten kan antas behöva registrera uppgifter om identiteten. Detta med hänsyn till att även om personen vistas utan tillstånd i Sverige har de allra flesta tidigare haft kontakt med Migrationsverket eller Polismyndigheten vid något tillfälle, exempelvis genom att utlänningen har ansökt om uppehållstillstånd. EES-medborgare som rest in från ett annat land i Schengenområdet kan dock behöva avvisas genom ett beslut av Polismyndigheten och personens identitetsuppgifter kan i samband med det behöva registreras av myndigheten.

Pass och nationella identitetskort får endast utfärdas till svenska medborgare. Det kan därför antas att i samband med utfärdande av dessa identitetshandlingar kommer en ny identitet i de flesta fall inte

[3] Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016.
[4] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.

att behöva registreras, utan det är fråga om att verifiera en sedan tidigare etablerad och, hos svenska myndigheter, registrerad identitet, och uppdatera uppgifterna i passregistret, bland annat den digitala ansiktsbild som tas upp vid ansökan. Detsamma kommer att gälla för det statliga identitetskort med resefunktion som föreslagits i promemorian *Ett statligt identitetskort*.[5] Om det behövs för att säkerställa att sökanden är svensk medborgare ska Polismyndigheten genomföra en utredning; om sökanden saknar svenskt personnummer eller samordningsnummer ska en utredning om medborgarskap alltid göras och Polismyndigheten ska då vid behov lämna en begäran till Skatteverket om att ett samordningsnummer tilldelas. Av Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort framgår att skäl att genomföra en utredning om medborgarskap till exempel kan vara att sökanden är eller har varit folkbokförd utomlands.[6]

Även om identiteten behöver verifieras i många andra situationer är det endast i de ärendeslag som vi redogjort för i kapitel 6 som det kan bli fråga om att registrera en helt ny identitet. I andra ärenden som Polismyndigheten, Migrationsverket och Skatteverket handlägger kan det i stället bli fråga om att uppdatera uppgifter om identiteteten i befintliga register.

8.2.2 Uppgifter från EU-gemensamma informationssystem

Vår bedömning

Alfanumeriska uppgifter om identitet som Polismyndigheten och Migrationsverket kan få tillgång till efter en sökning i SIS, VIS, in- och utresesystemet eller CIR för att identifiera en person får behandlas i den centrala utlänningsdatabasen.

Av avsnitt 7.4.3 framgår att Migrationsverket och Polismyndigheten kan söka i EU-gemensamma informationssystem både för att verifiera identitet och identifiera en person i olika ärendeslag. Uppgifter som då kan inhämtas från in- och utresesystemet, Schengens informationssystem (SIS), Informationssystemet för viseringar (VIS) och EU:s

[5] Ju2026/01595.
[6] 3 kap. 6 § PMFS 2021:3, FAP 530-1.

gemensamma databas för identitetsuppgifter (CIR) kan i olika utsträckning behöva registreras i den centrala utlänningsdatabasen (se närmare om detta i avsnitt 8.3.1). För att detta ska vara möjligt behöver behandlingen vara tillåten dels enligt dataskyddsförordningen[7] och utlänningsdatalagen, dels enligt de relevanta förordningar som reglerar tillgången till det aktuella informationssystemet på EU-nivå. Förordningarna innehåller särskilda bestämmelser som på olika sätt kan begränsa hur uppgifter som har inhämtats från respektive informationssystem får behandlas. I följande tabell ges en översikt av de bestämmelser i relevanta EU-förordningar som kan aktualiseras vid inhämtning av uppgifter från nämnda system.

Tabell 8.1 Stöd för att hämta in uppgifter

Ärendeslag	System	Reglering
Inre utlänningskontroller Gränskontroller Ansökan om uppehållstillstånd (ej internationellt skydd)	In- och utresesystemet	Artikel 28 i in- och utreseförordningen
Inre utlänningskontroller Gränskontroller Viseringsärenden	VIS	Artikel 30 i VIS-förordningen[1]
Inre utlänningskontroller Gränskontroller Ansökningar om internationellt skydd	SIS	Artikel 41 i gränsförordningen[2]
Inre utlänningskontroller Gränskontroller Ansökningar om internationellt skydd	CIR	Artikel 18 och 20 i IOF[3]

[1] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008.
[2] Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018.
[3] Europaparlamentets och rådets förordningar (EU) 2019/817 och (EU) 2019/818 av den 20 maj 2019.

Vårt uppdrag omfattar inte att närmare analysera om det finns ett behov av författningsändringar för att Polismyndigheten och Migrationsverket ska kunna registrera uppgifter som inhämtats från dessa EU-gemensamma system i den centrala utlänningsdatabasen. Sådana överväganden har, i varierande utsträckning, gjorts inom ramen för tidigare lagstiftningsärenden angående behov av anpassning av svensk rätt till relevanta förordningar. Exempelvis gjordes i promemorian

[7] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

Anpassning av svensk rätt till EU:s nya in- och utresesystem bedömningen att artikel 28 i in- och utreseförordningen – som anger att uppgifter som inhämtats från in- och utresesystemet enligt bland annat artikel 26 (verifiering av identiteten) och 27 (identifiering) får lagras i nationella register – är direkt tillämplig och att den inte hindrar att uppgifter som inhämtats från systemet behandlas för andra ändamål än insamlingsändamålet, om detta är förenligt med dataskyddslagstiftningen; de allmänt hållna förutsättningarna för lagring som ställs upp i artikel 28 bedömdes i allt väsentligt motsvara vad som redan gäller för behandling av personuppgifter enligt dataskyddsförordningen och utlänningsdatalagen.[8]

När det gäller alfanumeriska uppgifter om identiteten är aktuella bestämmelser, enligt vår bedömning, endast tillämpliga när en identifiering har gjorts, inte vid en verifiering av identiteten. I det senare fallet kan uppgifterna om identiteten nämligen inte anses ha hämtats från systemet utan från den enskilde.[9] Även vid en identifiering som görs genom att biometriska uppgifter används för att få en träff i systemet, från vilket alfanumeriska uppgifter kan inhämtas, kan det enligt vår bedömning ifrågasättas om bestämmelserna om lagring i nationella system kan anses tillämpliga på alfanumeriska identitetsuppgifter, av följande skäl. För det första innehåller förordningarna bestämmelser som uttryckligen ger stöd för att identifiera en person, vilket syftar till att den myndighet som genomför sökningen ska få information om vem personen är, och utifrån detta vidta relevanta åtgärder enligt förordningen. Att uppgifter om identitet som myndigheten får vid en träff inte skulle få behandlas i ett nationellt register – om detta är tillåtet enligt dataskyddsförordningen och eventuella nationella registerförfattningar – framstår inte som rimligt, då det skulle omintetgöra syftet med identifieringsmekanismen. För det andra bör det hållas i minnet att identifieringen av en person inte är ett ändamål i sig utan att det tjänar ett specifikt syfte, exempelvis att Polismyndigheten ska kunna ta ställning till om en person har rätt att vistas i Sverige.[10] Uppgifterna om identiteten är alltså normalt nödvändiga för att kunna handlägga det ärende som föranlett att myn-

[8] *Anpassning av svensk rätt till EU:s nya in- och utresesystem*, Ds 2021:9, s. 89. Se även *Anpassning av svensk rätt till den reviderade VIS-förordningen*, prop. 2024/25:176, s. 43.
[9] Ds 2021:9, s. 119.
[10] Se yttrande från Europeiska datatillsynsmannen (EDPS), *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, den 16 april 2018.

digheteten har sökt i ett visst EU-gemensamt informationssystem. Om uppgifterna om identitet som den kontrollerande myndigheten får tillgång till genom identifiering inte skulle få behandlas i den centrala utlänningsdatabasen – på grund av begränsningar i den relevanta förordningen – skulle dessa helt centrala uppgifter saknas i den dossier som skapas av Migrationsverket eller Polismyndigheten, i till exempel ett ärende om avvisning. För det tredje kan vi konstatera att de EU-gemensamma systemen innehåller vissa särskilda uppgifter, som är *kopplade* till en viss identitet; exempelvis innehåller SIS information om den enskilde är våldsbenägen och anledningen till ett tidigare beslut om nekad inresa. Att särskilda begränsningar gäller för hur sådana uppgifter får behandlas, vilka kan vara specifika för ett visst system, är däremot naturligt.

Sammantaget anser vi att de begränsningar som finns för behandling av uppgifter från SIS, VIS, in- och utresesystemet och CIR inte bör uppfattas som att de hindrar att uppgifter om identitet som den kontrollerande myndigheten får tillgång till i systemet genom identifiering får behandlas i den centrala utlänningsdatabasen, så länge det är förenligt med dataskyddsförordningen och utlänningsdatalagen. Dessa uppgifter bör också kunna registreras i ett sådant nationellt identitetsindex som vi redogör för i kapitel 11–18. Den behandling av uppgifter som i sådana fall skulle ske kan inte grunda sig på utlänningsdatalagen, eftersom behandlingen då görs för andra ändamål än de som anges i den lagen, utan förutsätter att kompletterande bestämmelser införs i nationell rätt som ger rättsligt stöd för sådan behandling.

8.3 Registrering av alfanumeriska uppgifter

I detta avsnitt redogör vi för befintligt och föreslaget författningsstöd för att, i olika register som Skatteverket, Migrationsverket och Polismyndigheten har tillgång till, registrera de alfanumeriska uppgifter om identiteten som tagits fram i ett visst ärende. Det kan även vara fråga om registrering av andra alfanumeriska uppgifter än identitetsuppgifter som är nära förknippade med personen eller ärendet, till exempel nummer på ett uppehållstillstånd eller födelseort. Vid en ansökan om uppehållstillstånd eller visering samt vid förvärv av svenskt medborgarskap görs registreringen av Migrationsverket i den centrala utlänningsdatabasen. I ärenden om folkbokföring och tilldelning av

samordningsnummer registrerar Skatteverket uppgifterna i folkbokföringsverksamheten och vid gränskontroller och inre utlänningskontroller registrerar Polismyndigheten, när det är aktuellt, alfanumeriska uppgifter om identiteten i den centrala utlänningsdatabasen. Vid en ansökan om svenskt pass eller ett nationellt identitetskort registrerar Polismyndigheten i dag identitetsuppgifter i passregistret och registret över nationella identitetskort. För att göra detta krävs en rättslig grund för att registrera – det vill säga behandla – uppgifterna, vilket vi redogör för i det följande.

8.3.1 Ärenden på utlänningsrättens område

När det gäller ärenden om uppehållstillstånd, visering och svenskt medborgarskap regleras vilka uppgifter som får lagras i utlänningsdatalagen. Detta framgår av 2 § i lagen. Enligt 3 § gäller lagen också vid Polismyndighetens verksamhet som rör utlänningars inresa och vistelse i Sverige och utresa eller avlägsnande från Sverige, det vill säga vid gränskontroller och inre utlänningskontroller. Personuppgifter får behandlas för de ändamål som framgår av 11 §. Av bestämmelsens första och andra punkt framgår att Migrationsverket, Polismyndigheten och utlandsmyndigheterna får behandla personuppgifter om det behövs för handläggning av ärenden i sådan verksamhet som avses i 2 och 3 §§ och vid kontroll av utlänningar i samband med inresa och utresa samt kontroll under vistelsen i Sverige.

Utlänningsdatalagen innehåller inte någon uttrycklig reglering av vilka kategorier av personuppgifter som får behandlas. Som skäl härför uttalades i förarbetena att den behandling som sker i verksamhet enligt utlännings- och medborgarskapslagstiftningen är omfattande och mångsidig och att det därför kan vara svårt och opraktiskt att specificera vilka kategorier av uppgifter som ska få behandlas. Ändamålsbestämmelserna ansågs i stället vara avgörande för vilka uppgifter som får behandlas.[11] Enligt vår mening får det anses givet att alfanumeriska uppgifter om identitet får registreras i den centrala utlänningsdatabasen med stöd av utlänningsdatalagen, eftersom sådana uppgifter är helt nödvändiga för att nämnda myndigheter ska kunna handlägga bland annat de ärenden där de ansvarar för att bestämma en grundidentitet. Utöver uppgifter om identiteten kan även andra uppgifter

[11] *Utlänningsdatalag*, prop. 2015/16:65, s. 78.

registreras i den dossier som skapas för varje individ när han eller hon för första gången blir aktuell i ett ärende hos Migrationsverket, exempelvis uppgifter om ansökningsdatum, resehandlingar, familjerelationer och beslut. Sådana uppgifter kan vara av betydelse för att lokalisera en unik träff i ett EU-gemensamt informationssystem, vid en sökning med alfanumeriska uppgifter. Om sådana särskilda uppgifter har inhämtats från exempelvis VIS eller in- och utresesystemet får de eventuella begränsningar som vi har redogjort för i avsnitt 8.2.2 beaktas.

I vissa ärenden ska Polismyndigheten och Migrationsverket registrera uppgifter i de EU-gemensamma systemen. Följande kan särskilt nämnas. Vid en gränskontroll ska Polismyndigheten, i enlighet med artikel 6 a i gränskodexen och artikel 14 och 16–18 i in- och utreseförordningen, uppdatera eller skapa en personakt i in- och utresesystemet för vissa kategorier av tredjelandsmedborgare, efter att identiteten verifierats. Identitetsuppgifter ska då föras in i personakten. Enligt artikel 8.1, 9 och 22a i VIS-förordningen ska en ansökningsakt skapas – i vilken bland annat uppgifter om identiteten ska föras in – vid en ansökan om Schengenvisering, nationell visering och uppehållstillstånd. I ärenden om inre utlänningskontroll, gränskontroll och uppehållstillstånd ska en registrering göras i SIS enligt artikel 24 i gränsförordningen om en tredjelandsmedborgare nekats inresa eller vistelse i Sverige, exempelvis när bedömningen gjorts att personen utgör ett hot mot allmän ordning (jfr MIG 2024:9). En sådan registrering får, enligt artikel 20.2 i gränsförordningen, innehålla bland annat identitetsuppgifter. Polismyndigheten sköter normalt alla registreringar i SIS, och är så kallat Sirenekontor. Slutligen kan nämnas att den reviderade Eurodacförordningen[12] innehåller bestämmelser som innebär att uppgifter om identiteten, men även biometriska underlag, avseende bland annat personer som ansöker om internationellt skydd ska föras över till och registreras i Eurodac.

8.3.2 Ärenden i folkbokföringsverksamheten

I ärenden om folkbokföring i samband med inflyttning till Sverige och vid tilldelning av samordningsnummer framgår det – i likhet med vad som gäller för utlänningsdatalagen – inte uttryckligen av folkbokföringsdatalagen (2026:126) vilka uppgifter som får behandlas i folk-

[12] Europaparlamentets och rådets förordning (EU) 2024/1358 av den 14 maj 2024.

bokföringsverksamheten. Detta skiljer sig mot den tidigare gällande lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, som innehöll en uppräkning av vilka uppgifter som fick behandlas i folkbokföringsdatabasen. En allmän förutsättning enligt den upphävda lagen var vidare att uppgifterna skulle röra en person som tilldelats ett person- eller samordningsnummer. I 2 kap. 3 § angavs vilka uppgifter som fick behandlas i folkbokföringsdatabasen, vilket bland annat inkluderade identitetsbeteckning – det vill säga personnummer eller samordningsnummer – samt namn, födelsetid och medborgarskap. Även andra uppgifter fick behandlas, bland annat civilstånd, adress, familjerelationer och födelseort. Det fanns däremot inte en möjlighet att exempelvis registrera information om personer som vistats olagligen i Sverige eller som är söker internationellt skydd, om de inte av någon anledning tidigare hade en identitetsbeteckning.

Folkbokföringsdatalagen innehåller inte någon bestämmelse som särskilt pekar ut vissa typer av uppgifter som får behandlas. Vidare innehåller folkbokföringsdatalagen en brett formulerad och flexibel ändamålsbestämmelse, som i förarbetena ansågs utgöra en betydande ändring i förhållande till nuvarande ordning.[13] Vilka uppgifter som får behandlas i folkbokföringsverksamheten begränsas alltså numera huvudsakligen genom att det i den primära ändamålsbestämmelsen i 5 § anges att Skatteverket får behandla personuppgifter om det är nödvändigt för att utföra verksamhet enligt 2 §, vilket omfattar bland annat folkbokföring och handläggning av ärenden om samordningsnummer. I 1 a § folkbokföringslagen respektive 1 kap. 2 § lagen om samordningsnummer anges däremot en uppräkning av vissa uppgifter som Skatteverket *ska* registrera.

I ärenden om folkbokföring och samordningsnummer saknas det möjligheter att inhämta identitetsuppgifter från EU-gemensamma system och det finns inte heller någon skyldighet att föra in sådana uppgifter i systemen.

[13] *Framtidens dataskydd vid Skatteverket, Tullverket och Kronofogdemyndigheten*, prop. 2025/26:88, s. 132.

8.3.3 Utfärdande av pass och nationellt identitetskort

Kontroll av identitet för svenska medborgare sker i många vardagliga sammanhang genom att den enskilde visar upp ett pass eller ett nationellt identitetskort. Vid utfärdandet av dessa handlingar behandlas sökandens identitetsuppgifter och biometriska uppgifter tas fram. Som vi återkommer till i kapitel 13 anser vi att dessa uppgifter bör kunna användas vid en registrering av en person i ett identitetsindex.

Svenskt pass utfärdas till svenska medborgare av passmyndigheten, vilket inom riket är Polismyndigheten. Utfärdandet regleras i passlagen (1978:302) och passförordningen (1979:664). Vid en ansökan om pass är sökanden skyldig att inställa sig personligen och ska enligt 6 § passlagen styrka sin identitet, sitt svenska medborgarskap och övriga personuppgifter. Polismyndigheten ska noggrant kontrollera sökandens identitet och sökanden ska i första hand styrka sin identitet genom att visa upp en godtagbar identitetshandling.[14] Identitetsuppgifter behandlas alltså regelmässigt i passärenden och registreras i passregistret som förs av Polismyndigheten, enligt 23 § passförordningen. Den rättsliga grunden för personuppgiftsbehandlingen i passverksamheten finns i första hand i artikel 6.1 e i dataskyddsförordningen (uppgift av allmänt intresse och myndighetsutövning). Passregistret är utformat som ett personregister och innehåller uppgifter om bland annat namn, personnummer, födelseort och kön, men även ansiktsbilder, dock inte i form av biometriska uppgifter, enligt gällande bestämmelser. Personuppgiftsbehandlingen bedömdes i departementspromemorian *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* innefatta en kartläggning av enskildas personliga förhållanden, även om syftet med behandlingen är ett annat. Passverksamheten i sig betraktas emellertid inte som särskilt integritetskänslig.[15] Trots detta finns det i dag ingen registerförfattning för passverksamheten. I promemorian *Ett statligt identitetskort* föreslås emellertid en ny pass- och identitetskortsdatalag med tillhörande pass- och identitetskortsdataförordning.[16] Enligt vår bedömning medför förslagen inte någon begränsning av hur uppgifter om identitet får registreras i det pass- och identitetskortsregister som föreslås, jämfört med vad som gäller för passregistret idag. I promemorian lämnas dock förslag om att biometriska uppgifter som tagits fram ur ansiktsbilden ska få lagras i pass-

[14] 3 kap. 1 och 2 §§ PMFS 2021:3 FAP 530-1.
[15] Ds 2019:5, s. 89 f.
[16] Ju2026/01595, s. 13 ff. och 33 ff.

och identitetskortsregistret, vilket skiljer sig från idag. Vi återkommer till det i avsnitt 8.4.3.

Det nationella identitetskortet regleras inte i lag utan i förordningen (2005:661) om nationellt identitetskort. Kortet utfärdas av passmyndigheten, det vill säga inom riket av Polismyndigheten. Den som ansöker om ett nationellt identitetskort ska enligt 2 § förordningen inställa sig personligen. Sökanden ska, i likhet med vad som gäller för pass, styrka sin identitet, sitt svenska medborgarskap och övriga personuppgifter, enligt 3 § förordningen. Enligt 14 § ska Polismyndigheten föra ett register över nationella identitetskort, vilket enligt 16 § ska innehålla uppgifter om bland annat namn och personnummer. Uppgifter om medborgarskap registreras inte. Det behövs av naturliga skäl inte eftersom identitetskortet endast utfärdas till svenska medborgare. Inte heller födelsetid registreras särskilt, men framgår normalt indirekt av personnumret. Registreringen av nationella identitetskort görs i praktiken i resehandlingssystemet RES. RES är ett kombinerat system som består av dels ett ärendehanteringssystem, dels uppgifter om utfärdade nationella identitetskort. RES innehåller alltså två olika uppgiftssamlingar när det gäller identitetskorten.[17] Enligt förslagen i promemorian *Ett statligt identitetskort* ska det nationella identitetskortet ersättas av ett statligt identitetskort. Den sökande ska, i likhet med vad som gäller för nationella identitetskort, styrka sin identitet. Enligt 11 § i förslaget till pass- och identitetskortsdatalag i promemorian ska Polismyndigheten, som vi nämnt ovan, föra ett pass- och identitetskortsregister. Registret kommer att innehålla bland annat identitetsuppgifter.[18]

8.4 Registrering av biometriska uppgifter

Enligt våra direktiv ska vi lämna förslag som främjar verifiering av identitet med grund i biometriska uppgifter, och undersöka lämpligheten med ett system med en unik identitetsnyckel. I kapitel 11–18 utvärderar vi hur grunderna för ett sådant system skulle kunna utformas. Tillgång till biometriska uppgifter är en grundläggande förutsättning för ett identitetsindex, och den upptagning av biometriska underlag som Skatteverket, Migrationsverket och Polismyndigheten kan

[17] *Ett säkert statligt id-kort – med e-legitimation*, SOU 2019:14, s. 252, 271 och 395.
[18] Ju2026/01595, s. 14 f. 75 och 171 f.

göra i olika ärendeslag skulle kunna utgöra ett viktigt moment om ett system med ett index skulle införas. I avsnitt 7.4.3 har vi redogjort för när biometriska underlag kan tas upp i olika ärendeslag där en grundidentitet kan behöva etableras. I detta avsnitt redogör vi för befintligt, beslutat och föreslaget författningsstöd för att kunna registrera biometriska underlag och biometriska uppgifter vid handläggningen av ett visst sådant ärende, men även vid en ansökan om pass och nationellt identitetskort samt det statliga identitetskort som har föreslagits.

Det bör här understrykas att den lagring av biometriska underlag och biometriska uppgifter som är möjlig i befintliga och föreslagna register *inte* utgör grund för att även registrera dessa uppgifter i ett nytt identitetsindex. En redogörelse av befintligt och föreslaget rättsligt stöd bör dock kunna tjäna som utgångspunkt för våra senare överväganden; att biometriska underlag och biometriska uppgifter lagras i olika befintliga ärenden redan i dag kan enligt vår bedömning vara en viktig indikator på att det kan finnas ett behov av att registrera dem även i syfte att kunna användas vid biometrisk verifiering av identitet mot ett identitetsindex.

8.4.1 Ärenden på utlänningsrättens område

Som vi anfört i avsnitt 8.3.1 innehåller utlänningsdatalagen inte någon precisering av vilka uppgifter som får behandlas med stöd av lagen. Behandling av fingeravtryck och fotografier regleras emellertid särskilt i 15 § utlänningsdatalagen. Enligt bestämmelsen får Migrationsverket föra separata register över fingeravtryck och fotografier som tas med stöd av vissa, i första stycket angivna, bestämmelser. I bestämmelsens andra stycke anges de ändamål som känsliga uppgifter som finns i registret får användas för. I dessa ändamål ingår bland annat prövning av ansökningar om uppehållstillstånd där skyddsbehov åberopas och inre utlänningskontroller.

I praktiken för Migrationsverket ett särskilt register över fingeravtryck. Fingeravtrycken lagras i ett separat register som Polismyndigheten har hand om åt Migrationsverket.[19] Fotografierna lagras däremot i den centrala utlänningsdatabasen, vilken ägs av och finns hos Migrationsverket. Även myndighetens samlade fotografier kan

[19] *Vissa identitetsfrågor inom utlänningsrätten*, prop. 2020/21:159, s. 21.

ses som ett register. Systemet är komplicerat och inte helt lätt att genomlysa.[20] Med hänsyn till syftet med detta avsnitt är det enligt vår mening inte nödvändigt att i detta sammanhang närmare redogöra för hur de biometriska underlag som får registreras i olika ärendeslag av Migrationsverket och Polismyndigheten hanteras administrativt och tekniskt, utan det är de rättsliga förutsättningarna som behöver belysas.

Som nämnts anges i 15 § första stycket utlänningsdatalagen under vilka förutsättningar som uppgifter i form av fingeravtryck och fotografier får registreras i relevanta register hos Migrationsverket. Av bestämmelsen framgår att fingeravtryck och fotografier som tagits med stöd av 9 kap. 8 och 8 h § utlänningslagen får registreras. Bestämmelsens ordalydelse ger enligt vår mening närmast intryck av att det endast är biometriska underlag som får lagras i Migrationsverkets register. Av andra stycket framgår samtidigt att ”uppgifter om fingeravtryck eller fotografier i registren” får användas för vissa angivna ändamål, vilket skulle kunna omfatta både biometriska underlag och de biometriska uppgifter som kan tas fram ur dem. Vi kan här notera att en liknande formulering används i 5 kap. 2 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område; i förarbetena till den bestämmelsen angavs uttryckligen att med uttrycket avsågs även biometriska uppgifter som tagits fram ur de biometriska underlagen, så kallade biometriska mallar, och att de biometriska mallarna i sig är uppgifter om de underlag som de har tagits fram ur.[21] Även om 15 § utlänningsdatalagen ger stöd för att lagra biometriska *uppgifter* i Migrationsverkets register över fingeravtryck och fotografier innebär det inte nödvändigtvis att så också sker i praktiken. Vi har dock under vårt arbete fått bekräftat av företrädare för Migrationsverket att myndigheten lagrar biometriska uppgifter som tagits fram ur fingeravtryck i registren. Däremot lagras inte biometriska uppgifter från fotografier som tagits upp med stöd av någon bestämmelse i 9 kap. utlänningslagen. Om fingeravtryck och ansiktsbild har tagits upp av Polismyndigheten ska myndigheten, enligt 6 kap. 14 § andra stycket utlänningsförordningen (2006:97), i de fall underlaget inte ska förstöras omedelbart, sända underlaget tillsammans med utredning i ärendet till Migrationsverket.

[20] *Personuppgiftsbehandling på utlännings- och medborgarskapsområdet*, SOU 2015:73, s. 277.
[21] *Biometri i brottsbekämpningen*, prop. 2024/25:37, s. 193.

I avsnitt 7.4.3 har vi redogjort för vilka ärenden som upptagning av biometriska underlag enligt 9 kap. 8 § utlänningslagen kan omfatta, nämligen ansökningar om internationellt skydd, gränskontroller och inre utlänningskontroller. När biometriska underlag tas upp med stöd av 9 kap. 8 § första stycket 1 och 4, krävs att utlänningen inte har kunnat styrka sin identitet eller att identiteten inte har kunnat klarläggas. Vid inre utlänningskontroller gäller dessutom, enligt 9 kap. 8 § andra stycket utlänningslagen, att det fotografi och de fingeravtryck som har tagits omedelbart ska förstöras om det kommer fram att utlänningen har rätt att vistas i Sverige. Att uppgifterna inte ska få lagras har motiverats av integritetshänsyn.[22] Fingeravtryck får enligt 9 kap. 8 § utlänningslagen i dess nuvarande lydelse, endast tas upp om personen har fyllt 14 år. Enligt en ändring i 15 § utlänningsdatalagen, som trädde i kraft i oktober 2025, ska även uppgifter som tagits upp med stöd av 9 kap. 8 h § utlänningslagen få lagras i Migrationsverkets register. Enligt nämnda bestämmelse får fingeravtryck och fotografier tas upp vid inre utlänningskontroll i syfte att genomföra en sökning i in- och utresesystemet. Genom det förslag om ändring av bestämmelsen som framgår av regeringens proposition *Anpassning av svensk rätt till den reviderade VIS-förordningen*[23] ska biometriska underlag också få tas upp för kontroll i VIS.

Mot denna bakgrund är det i praktiken i relativt få fall, förutom vid ansökningar om internationellt skydd, som biometriska underlag och biometriska uppgifter i praktiken kan lagras i Migrationsverkets register. När det gäller ärenden om svenskt medborgarskap saknas i nuläget helt möjligheter att ta upp eller registrera biometriska underlag eller biometriska uppgifter som har tagits fram ur dem. Fingeravtryck och fotografier som har tagits upp vid en ansökan om visering vid svenska myndigheter kan inte heller registreras nationellt.

I vissa ärendeslag ska de biometriska underlag som tas upp med stöd av bestämmelser i 9 kap. utlänningslagen registreras i relevanta EU-gemensamma system. Här kan följande särskilt nämnas. Enligt artikel 22a jämfört med 22c-22f i VIS-förordningen ska biometriska uppgifter registreras i VIS vid en ansökan om uppehållstillstånd. Bestämmelserna är direkt tillämpliga och det ankommer på Migrationsverket att iaktta de begränsningar för registrering av underårigas upp-

[22] Se bland annat *Anpassning av svensk rätt till EU:s nya in- och utresesystem*, prop. 2021/22:81, s. 50 f.
[23] Prop. 2024/25:176, s. 74 f.

gifter som följer av artikel 22a.2 i VIS-förordningen, bland annat om att fingeravtryck från barn under sex år inte får föras in i VIS-systemet.[24] För personer som ansöker om internationellt skydd ska fingeravtryck för personer som har fyllt 14 år som tas upp vid ansökan registreras i Eurodac. Genom den reviderade Eurodacförordningen sänks åldern till sex år och registreringen av biometriska underlag utökas till att avse även ansiktsbilder, enligt artikel 17.1 i förordningen. Uppgifterna ska sparas dels i det centrala systemet, dels i CIR, enligt artikel 3.2 i den reviderade Eurodacförordningen.

Föreslagna ändringar

De begränsningar som finns när det gäller att kunna lagra biometriska underlag och biometriska uppgifter i olika ärenden på utlänningsrättens område har uppmärksammats i flera lagstiftningsärenden och det har lämnats förslag på ändringar i utlänningslagen och utlänningsdatalagen som tillsammans syftar till att göra det möjligt att registrera sådana uppgifter i fler fall än i dag.

Vid en ansökan om uppehållstillstånd kan biometriska underlag tas upp både med stöd av 9 kap. 8 § och 8 a § utlänningslagen. Sistnämnda bestämmelse är tillämplig oavsett vilken grund för ansökan som åberopas av utlänningen. En väsentlig begränsning i dess nuvarande lydelse är att fingeravtrycken och de biometriska uppgifter som tas fram ur dem och ur fotografiet omedelbart ska förstöras när Migrationsverket skiljer ärendet från sig. I regeringens proposition *Stärkt återvändandeverksamhet* har därför förslag lämnats som innebär att uppgifter om fingeravtryck och fotografier från samtliga ansökningar om uppehållstillstånd ska kunna lagras i Migrationsverkets register över fingeravtryck och fotografier, för att minska risken för identitetsbedrägerier. Förslag lämnades vidare om att grunderna för att ta upp fingeravtryck och fotografier i samband med en ansökan om uppehållstillstånd ska vara samlade i 9 kap. 8 a § utlänningslagen och att regleringen i tredje stycket om att de biometriska underlagen och de biometriska uppgifter som kan tas fram ur dessa ska förstöras när ärendet avgörs ska upphävas.[25] De föreslagna ändringarna möjliggör alltså att biometriska underlag och biometriska uppgifter som tas upp

[24] Prop. 2024/25:176, s. 35 f.
[25] Prop. 2025/26:263, s. 123 ff. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.

och fram i ärenden om uppehållstillstånd kan registreras i betydligt större utsträckning än i dag.

När det gäller ärenden om nationell visering har förslag lämnats om att en ny bestämmelse, 9 kap. 8 j §, ska införas i utlänningslagen som innebär att biometriska underlag ska tas upp vid en ansökan om nationell visering, och att dessa och de biometriska uppgifter som kan tas fram ur dem ska få registreras i Migrationsverkets register, genom att 15 § första stycket utlänningsdatalagen ändras på så sätt att den även omfattar den föreslagna bestämmelsen. Motivet till förslagen är att en nationell visering, på grund av sin giltighetstid och sitt användningsområde, närmast är att jämföra med uppehållstillstånd för besök eller andra tillfälliga uppehållstillstånd med kort giltighetstid och att en möjlighet att registrera och jämföra biometriska uppgifter skulle öka möjligheterna för svenska myndigheter att fastställa identiteten på en utlänning som påträffas i Sverige och som inte kan styrka sin identitet eller rätt att vistas i landet.[26]

I nuläget saknas, som nämnts ovan, möjlighet att ta upp eller registrera biometriska underlag och biometriska uppgifter i ärenden om svenskt medborgarskap. Enligt lämnade förslag ska emellertid en sådan möjlighet införas, genom att en ny bestämmelse, 13 f §, införs i lagen om svenskt medborgarskap och att den tas upp i 15 § första stycket utlänningsdatalagen, i en ny nionde punkt. Fingeravtryck och fotografi ska enligt förslagen få lagras i Migrationsverkets register endast om en verifiering av dem visar att de biometriska uppgifter som kan tas fram ur dem inte stämmer överens med tidigare registrerade uppgifter eller om uppgifter inte tidigare registrerats. Om verifieringen visar att det är samma person som tidigare har ansökt om uppehållstillstånd finns dessa uppgifter nämligen redan lagrade i Migrationsverkets register.[27]

Slutligen kan här nämnas att såväl Migrationsverket som Polismyndigheten kan behöva fatta beslut om avvisning, till exempel vid en inre utlänningskontroll om det kommer fram att personen inte har rätt att vistas i Sverige. Biometriska underlag kan i dag inte tas upp i ett ärende om avvisning eller utvisning. Enligt förslag som lämnats i regeringens proposition S*tärkt återvändandeverksamhet* ska en sådan möjlighet införas i 9 kap. 8 § 5 utlänningslagen och underlaget och de biometriska uppgifter som kan tas fram ur dem kommer då

[26] Prop. 2024/25:176, s. 35 ff.
[27] Prop. 2025/26:263, s. 129 ff.

att kunna registreras i Migrationsverkets register, med stöd av 15 § utlänningsdatalagen.[28]

8.4.2 Ärenden i folkbokföringsverksamheten

Fingeravtryck, ansiktsbilder och biometriska uppgifter som tas fram ur dessa får behandlas i folkbokföringsverksamheten med stöd av bestämmelserna i 5 och 8 §§ folkbokföringsdatalagen. En förutsättning är emellertid att behandlingen är nödvändig för att utföra verksamhet enligt 2 §, vilket omfattar bland annat folkbokföring och handläggning av samordningsnummer, samt att den är nödvändig med hänsyn till ändamålet med behandlingen. Det finns alltså rättsligt stöd för att behandla sådana uppgifter i folkbokföringsverksamheten. Enligt 26 c § andra stycket folkbokföringslagen och 2 kap. 4 § andra stycket lagen om samordningsnummer ska de biometriska underlag som tagits upp vid en identitetskontroll enligt respektive bestämmelse emellertid omedelbart förstöras efter att kontrollen har genomförts. Detsamma gäller de biometriska uppgifter som tagits fram ur underlagen. Det saknas alltså enligt gällande bestämmelser en möjlighet att lagra biometriska underlag eller biometriska uppgifter för användning vid ett senare tillfälle.

I ärenden om folkbokföring vid födelse i Sverige saknas möjligheter att ta upp såväl fingeravtryck som ansiktsbild från den enskilde. Ett fotografi av en nyfödd torde enligt vår bedömning inte ha något värde som biometriskt underlag, varför behov av att registrera sådant underlag saknas. Det finns vanligtvis inte heller några frågetecken kring barnets identitet som behöver eller kan avhjälpas med upptagning av biometriska underlag.

Syftet med att Skatteverket ska kunna göra en identitetskontroll och då ta upp biometriska underlag bland annat i ärenden om folkbokföring vid inflyttning och tilldelning av samordningsnummer är att stärka kontrollen vid handläggningen av dessa ärenden.[29] Som vi redogjort för ovan får uppgifterna däremot inte registreras efter att kontrollen gjorts. I betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* konstaterades att en möjlighet att registrera uppgifterna skulle avsevärt minska risken för att en enskild registreras

[28] Prop. 2025/26:263, s. 126 ff.
[29] *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 44 f. och *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 65.

under flera identiteter och för att en enskild, som utnyttjar en annan persons identitet, ändrar identitetsuppgifter i den utnyttjade identiteten för att minska risken för upptäckt vid användandet. Förslag har därför lämnats i propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* dels om att 26 c § andra stycket folkbokföringslagen och 2 kap. 4 § andra stycket lagen om samordningsnummer ska ändras, dels om att nya punkter ska införas i 1 a § 18 folkbokföringslagen och 1 kap. 2 § andra stycket 12 lagen om samordningsnummer, som ger Skatteverket stöd för att i vissa ärenden om folkbokföring och tilldelning av samordningsnummer registrera dels ansiktsbilder och fingeravtryck, dels de biometriska uppgifter som tas fram ur dessa.[30]

8.4.3 Utfärdande av pass och nationellt identitetskort

Den som ansöker om pass är, som vi redogjort för ovan, skyldig att låta Polismyndigheten ta hans eller hennes fingeravtryck och en ansiktsbild i digitalt format. För barn under sex år och personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck gäller inte skyldigheten att lämna fingeravtryck. Ansiktsbilden registreras i passregistret. Det är emellertid endast det biometriska underlaget som registreras, inte de biometriska uppgifter som tagits fram ur ansiktsbilden; av 6 a § passlagen framgår att de omedelbart ska förstöras när passet har lämnats ut. Av samma bestämmelse följer att fingeravtrycken och tillhörande biometriska uppgifter ska förstöras vid samma tidpunkt. I förarbetena till passlagen uttalades att det inte skulle vara möjligt att bygga upp ett separat fingeravtrycksregister med hjälp av de fingeravtryck som lämnas vid passansökningar.[31] I nuläget lagras alltså inga biometriska uppgifter i passregistret vid en ansökan om pass utan biometriska underlag i form av ansiktsbild och fingeravtryck lagras endast i det chip som finns i passhandlingen. Vid en ansökan om nationellt identitetskort ska en kopia av den ansiktsbild som tas upp lagras i Polismyndighetens register över sådana kort, enligt 16 § 3 förordningen om nationellt identitetskort. I övrigt ska fingeravtryck och biometriska uppgifter förstöras efter att kortet har lämnats ut eller, om kortet inte har lämnats ut, när det har gått 90 dagar

[30] Prop. 2025/26:261, s. 47 ff.
[31] *Fingeravtryck i pass*, prop. 2008/09:132, s. 12 f. och 16.

från den dag då det utfärdades, i enlighet med 4 § förordningen. Det registreras alltså, på samma sätt som vid ansökan om pass, inte några biometriska uppgifter i dessa ärenden i nuläget. Förslag har emellertid lämnats i promemorian *Ett statligt identitetskort* om att det nationella identitetskortet ska ersättas av ett nytt statligt identitetskort och att ansiktsbilden och de biometriska uppgifter som tas fram ur denna – i samband med både ansökan om pass och om statligt identitetskort – ska sparas i det pass- och identitetskortsregister som också föreslogs.[32] När det gäller fingeravtryck och de biometriska uppgifter som kan tas fram ur dessa föreslogs emellertid inga förändringar.[33]

[32] Ju2026/01595, s. 14 f. och 171.
[33] Ju2026/01595, s. 130 ff.

9 Identitetsmissbruk – orsaker och konsekvenser

9.1 Inledning

I takt med en ökad digitalisering av samhället och en ökad rörlighet för personer såväl inom EU som globalt har behovet av en säker och tillförlitlig kontroll och förvaltning av identitet blivit allt tydligare. Som lyftes fram i delbetänkandet *En säker och tillgänglig statlig e-legitimation* finns det många fördelar med ett alltmer digitaliserat samhälle, men det finns också en tydlig baksida i form av den identitetsrelaterade brottslighet som kan begås bland annat genom att använda falska eller olovligt åtkomna identitetshandlingar.[1] Brister i kontrollen av identitet i olika delar av samhället utnyttjas dels på individnivå, dels av den organiserade brottsligheten, exempelvis genom att multipla identiteter används för att på felaktiga grunder få tillgång till ekonomiska förmåner från välfärdssystemen. Åtminstone hälften av bedrägeribrotten i Sverige bedöms inkludera identitetsmissbruk, vilket benämns som id-fusk, id-kapning, identitetsstöld och identitetsbaserad brottslighet. Missbruket sker ofta i sammanhang som kreditkortsbedrägerier, målvaktsupplägg, välfärdsbrott, svartarbete eller penningtvätt.[2] I detta kapitel belyser vi dessa frågor.

9.2 Problembild

Att utge sig för att vara någon annan – oavsett om personen existerar eller inte – är ett centralt moment vid många bedrägerier. Brister i myndigheternas kontrollmöjligheter leder till att individer kan miss-

[1] SOU 2023:61, s. 109.
[2] *Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen*, SOU 2020:35, s. 143 ff.

bruka falska eller multipla identiteter, vilket påverkar såväl rättsstaten som tilliten till välfärdssystemet. Utredningen om samordning av statliga utbetalningar från välfärdssystemen konstaterade att genom att missbruka identiteter kan en brottsling skapa förutsättningar för att begå brott, minska risken för upptäckt, utvidga sin brottslighet samt minska möjligheterna till rättsskipning. Motivet till identitetsmissbruk är ofta ekonomisk vinning, men kan också vara att den enskilde kan få en viss anonymitet som kan innebära en frihet från samhällets förpliktelser, exempelvis för att kunna undgå att betala skatt eller ta ansvar för en trafikförseelse.[3] Ett övergripande problem när det gäller framför allt organiserad brottslighet är att lagstiftning och kontrollsystem till stor del är nationellt begränsade och inte dimensionerade för eller anpassade till en gränsöverskridande brottslighet, i synnerhet när den bygger på missbruk av identitet, vilket försvårar att spåra brottsligheten; i detta har den fria rörligheten för unionsmedborgare inom EU, men även utformningen av exempelvis regelverket kring arbetstillstånd i Sverige, en bidragande roll.

I detta avsnitt beskriver vi den problembild avseende identitetsmissbruk som har växt fram på olika områden.

9.2.1 Översikt av olika typer av identitetsmissbruk

Identitetsmissbruk förekommer i flera olika former, men de typer som genomgående har lyfts fram i tidigare förarbeten och rapporter är att uppgifter om identiteten är falska eller felaktiga, vilket kan innebära att en individ förekommer under multipla identiteter hos olika myndigheter, eller att identiteter utnyttjas på olika sätt.

Med *felaktig identitet* menas att uppgifterna om identiteten inte stämmer överens med personens verkliga förhållanden. Det kan till exempel röra sig om att en person som ansöker om internationellt skydd gör gällande att han eller hon är ett barn, trots att personen är vuxen, men att korrekta uppgifter lämnas i övrigt, om namn och medborgarskap. En felaktig identitet behöver inte uppstå som resultat av ett uppsåtligt handlande av den enskilde. En *falsk identitet* kan skapas genom att den enskilde medvetet använder förfalskade eller manipulerade identitetshandlingar vid en ansökan om exempelvis uppehållstillstånd. Till falska identiteter räknas även vissa fall av

[3] SOU 2020:35, s. 146.

look-a-like-identiteter, det vill säga de fall där en person visar upp en äkta identitetshandling som är utfärdad för en annan person. Med falsk identitet menas vanligen att det inte finns någon korrekt identitet överhuvudtaget och att det helt saknas korrekta uppgifter som kan ersätta de felaktiga.[4]

Vid *multipla identiteter* är en, flera eller samtliga av de registrerade identiteterna falska eller felaktiga. Multipla identiteter kan skapas på olika sätt och i praktiken innebära att en person har tilldelats mer än ett samordningsnummer eller folkbokförts mer än en gång med olika identitetsuppgifter. Det kan också avse en situation då en person har samordningsnummer eller personnummer parallellt i två eller flera identiteter. Även vid kontakter med Migrationsverket kan en person ha uppträtt under olika identiteter och vara registrerad med mer än en identitet.

När det gäller *utnyttjade identiteter* kan det exempelvis ske genom att en person lämnar över sina personuppgifter till någon annan, och då ofta utan insikt om i vilken omfattning eller i vilket sammanhang uppgifterna kommer att användas. Överlämningen kan ske under hot, men även frivilligt. Om en person medvetet, eventuellt mot betalning, lånar ut sina identitetsuppgifter kan det ofta vara fråga om att han eller hon agerar som en så kallad målvakt.[5] En utnyttjad identitet behöver alltså inte vara falsk eller felaktig. I begreppet ryms även så kallade *kapade identiteter*, det vill säga när en persons identitet används av en obehörig person utan den förste personens samtycke.[6] Detta är sedan år 2016 kriminaliserat genom bestämmelsen om olovlig identitetsanvändning i 4 kap. 6 b § brottsbalken.

9.2.2 Felaktiga och falska identiteter

En felaktig eller falsk identitet skapas vanligtvis inom ramen för de ärenden som vi redogjort för i kapitel 6, det vill säga situationer när en person har kontakt med svenska myndigheter för första gången, exempelvis i samband med en ansökan om uppehållstillstånd. En felaktig eller falsk identitet kan även skapas vid utfärdandet av en identitetshandling. Som framgår av betänkandet *Folkbokförings-*

[4] Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter*, RiR 2024:12, s. 20 och *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 407.
[5] SOU 2023:61, s. 110.
[6] SOU 2025:75, s. 408.

verksamhet, biometri och brottsbekämpning har Skatteverket framhållit att risken för fel är störst när en enskilds identitet första gången ska etableras i landet, det vill säga bland annat i samband med fastställande av ett personnummer eller tilldelning av ett samordningsnummer.[7] En tillförlitlig verifiering av identiteten är av helt avgörande betydelse i detta skede, eftersom den identitet som då registreras kommer att ligga till grund för beslut av andra myndigheter, exempelvis vid en ansökan om en socialförsäkringsförmån som handläggs av Försäkringskassan. Det är inte möjligt att alltid med säkerhet spåra en persons identitet innan han eller hon kommer i kontakt med svenska myndigheter för första gången, men i samband med att en registrering av identiteten görs i Sverige måste ambitionen alltid vara att skapa en så säker koppling som möjligt mellan en person och en identitet. Ett citat från en myndighetsrepresentant ur Brottsförebyggande rådets rapport från år 2016 om bedrägeribrottsligheten i Sverige beskrev problemet med falska och felaktiga identiteter vid den tidpunkten enligt följande:

> Vi har ju oftast en identitet på ett papper, och vi vet ju inte ens om det finns någon person bakom, det kan vara ett luftslott.[8]

En falsk identitet innebär att det finns någon form av uppsåt hos den enskilde att vilseleda svenska myndigheter om sin identitet. De oriktiga uppgifterna grundar sig ofta i att han eller hon använder förfalskade identitetshandlingar. I ärenden om uppehållstillstånd kan det finnas svårigheter med att bekräfta äktheten av utländska identitetshandlingar, då det kan saknas ett tillförlitligt referensmaterial som gör det möjligt att kontrollera att ett visst dokument är utfärdat på rätt sätt. En effektiv granskning av utländska identitetshandlingar kan kräva tillgång till särskild teknisk utrustning och kompetens, i synnerhet för att myndigheten ska kunna upptäcka medvetet förfalskade eller förvanskade handlingar. I avsnitt 7.4.2 har vi redogjort för de tekniska metoder som de kontrollerande myndigheterna använder sig av för att granska olika handlingar, bland annat användning av lupp, UV-lampor och mikroskop. Migrationsverket har även möjlighet att göra en mer grundlig dokumentgranskning med hjälp av certifierade dokumentgranskare som förfogar över mer avancerade verktyg, om det finns anmärkningar eller avvikelser vid den första

[7] SOU 2025:75, s. 409.
[8] Brå, Rapport 2016:9, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag*, s. 150.

kontrollen. Med detta sagt kan vi konstatera att en gemensam riskfaktor utgörs av att möjligheten att upptäcka falska eller manipulerade identitetshandlingar – i vart fall andra än passhandlingar som är försedda med maskinläsbara säkringar och biometriska kännetecken – till stor del är avhängig av den enskilde tjänstemannens utbildningsnivå i fråga om dokumentgranskning och individuell erfarenhet. Dessa brister har lyfts fram i Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter*; bedömningen gjordes att det saknas tillräcklig kompetens och utbildning hos de kontrollerande myndigheterna för att säkerställa att korrekta identiteter fastställs i grundärendena och att tillgång till teknisk utrustning skiljer sig åt.[9] Även arbetsbördan vid ett givet tillfälle kan enligt vår mening antas påverka.

Förutsättningarna för att skapa en falsk eller felaktig identitet i Sverige kan antas vara mindre i de ärenden där ett krav för att ansökan ska beviljas är att sökanden kan styrka sin identitet, vilket normalt ska göras genom uppvisande av ett giltigt hemlandspass. En sådan handling kan äkthetsgranskas och är svårare att manipulera eftersom den vanligtvis innehåller säkringar av olika slag. Det finns även ett bra referensmaterial att tillgå för de kontrollerande myndigheterna. Som vi beskrivit i avsnitt 7.4.2 har myndigheterna, beroende på ärendeslaget, också vissa möjligheter att ta upp biometriska underlag för att, med de biometriska uppgifter som kan tas fram ur underlaget, göra en en-till-en-jämförelse med uppgifter som finns lagrade i ett pass som utlänningen har åberopat till stöd för sin identitet. Användning av biometriska uppgifter är ett effektivt sätt att motverka missbruk av identitetshandlingar, vilket har lyfts fram bland annat av 2017 års ID-kortsutredning.[10] De kontrollerande myndigheterna har också en möjlighet att vidta vissa tvångsåtgärder för att få tillgång till identitetshandlingar som den enskilde undanhåller, vilket dock i första hand kan antas få betydelse vid inre utlänningskontroller och i ärenden om uppehållstillstånd på grund av behov av internationellt skydd, det vill säga sådana ärenden där det kan finnas ett incitament för den enskilde att lämna felaktiga eller falska uppgifter om identiteten.

Att en sökande visar upp en godtagbar identitetshandling utesluter inte att en felaktig eller falsk identitet kan komma att etableras

[9] RiR 2024:12, s. 97.
[10] *Ett säkert statligt ID-kort – med e-legitimation*, SOU 2019:14, s. 292.

i Sverige. Även om en åberopad handling innehåller säkringar och bedöms som äkta kan underlaget för de identitetsuppgifter som framgår av handlingen vara felaktigt. Som exempel kan nämnas maskinläsbara afghanska hemlandspass, där det underlag som ligger till grund för passhandlingen ofta utgörs endast av en så kallad tazkira, en handling som är av mycket enkel kvalitet och i praxis från Migrationsöverdomstolen har ansetts i princip sakna bevisvärde (se MIG 2014:1). Detta trots att hemlandspass normalt anses styrka identiteten i ett ärende om uppehållstillstånd. En identitetshandling kan vidare ses som endast en form av ögonblicksbild av innehavaren vid en viss tidpunkt – ofta då handlingen utfärdades – och säger inte något om senare händelser som är av betydelse för att kunna verifiera identitet hos innehavaren; handlingen kan vara återkallad eller på annat sätt ha förlorat sin giltighet utan att detta med lätthet upptäcks av svenska myndigheter. Det kan också förekomma att en äkta handling manipuleras på olika sätt, exempelvis genom att endast vissa uppgifter om identiteten ändras eller att ansiktsbilden byts ut. Pass som innehåller säkringar och biometriska uppgifter kan emellertid antas vara svåra att förfalska och manipulera på detta sätt.[11]

I vissa fall används stulna utländska, i sig äkta, pass och andra typer av identitetshandlingar för att skapa nya, falska, identiteter i Sverige.[12] Det är då fråga om så kallade look-a-likes, det vill säga att personen som visar upp passet är tillräckligt lik den som passet tillhör för att detta inte ska upptäckas; som vi noterat i avsnitt 7.4.2 kan det mänskliga ögat sällan med säkerhet avgöra att det är samma person på ett foto som den som står framför en.[13] Bedrägerier som utförs med hjälp av äkta handlingar kan därför vara svåra att upptäcka och bekämpa. I Riksrevisionens ovan nämnda rapport framkommer att ett pass som är tekniskt äkta men utfärdat i fel identitet svårligen skulle upptäckas vid en gränskontroll.[14]

Felaktiga och falska identiteter kan alltså uppstå genom att brister i åberopade identitetshandlingar inte upptäcks. Konsekvenserna kan i viss mån anses vara särskilt svåra för samhället i dessa fall, eftersom identiteten har ansetts vara styrkt med en tillförlitlig identitetshandling när den etablerades och kan komma att åberopas av den enskilde även i andra sammanhang.

[11] *Åtgärder mot missbruk av svenska pass*, prop. 2015/16:81, s. 8.
[12] Brå, Rapport 2016:9, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag*, s. 150.
[13] *Om folkbokföring, samordningsnummer och identitetsnummer*, SOU 2021:57, s. 232.
[14] RiR 2024:12, s. 44 och 51.

Risken i sig för att felaktiga eller falska identiteter uppstår får enligt vår mening anses högre i ärendeslag där krav på styrkt identitet inte kan upprätthållas. För den som vill undanhålla sin korrekta identitet saknas då incitament att på eget initiativ lämna över eventuella identitetshandlingar som han eller hon innehar. Även om grundkravet är att identiteten ska vara styrkt tillämpas i praktiken ett lägre beviskrav i vissa ärenden om uppehållstillstånd, i första hand när grunden är behov av internationellt skydd men även vid ansökan om familjeåterförening eller när uppehållstillstånd beviljas på grund av synnerligen ömmande omständigheter. Vid ansökningar om internationellt skydd är identitetsfrågan ofta av underordnad betydelse, med hänsyn dels till att skyddsbehovet inte behöver vara kopplat till identiteten utan kan bero på en viss faktisk hotbild eller på att personen kommer från ett visst område, dels till att ett lägre beviskrav – sannolikt – gäller som utgångspunkt i sådana ärenden. I sådan ärenden saknas ofta en passhandling (se avsnitt 7.4.2) och muntliga uppgifter om identiteten kan därför få en avgörande betydelse. Dessa kan vara svåra att kontrollera och kommer ofta att accepteras, och läggs då till grund för den identitet som registreras av Migrationsverket i ärendet. Det bör understrykas att det inte behöver vara fråga om falska uppgifter, utan den som ansöker om internationellt skydd kan lämna uppgifter som han eller hon är övertygad om är korrekta, men som i sin tur bygger på muntliga uppgifter från anhöriga eller handlingar från hemlandet som inte i sig är tillförlitliga. Fel kan även i vissa fall tänkas bero på språkförbistring vid tolkning eller felaktiga bedömningar vid en språkanalys, som medför att en person tillskrivs en hemvist och ett medborgarskap som inte är korrekt. Det behöver inte heller vara fråga om att alla delar av identiteten är felaktiga, utan det kan exempelvis röra sig om att en vuxen person utger sig för att vara barn. En sådan felaktig identitetsuppgift kan få stora följdeffekter – oavsett om den beror på medvetet falska uppgifter eller på att den enskilde inte har kännedom om sin rätta ålder – i form av att den enskilde åläggs skyldigheter eller ges rättigheter som är knutna till en viss ålder. Som exempel kan nämnas straffmyndighet, rätt till vård och skolgång samt värnplikt och rätt att framföra motorfordon.

Vid förvärv av medborgarskap genom naturalisation kan ett lägre beviskrav också tillämpas under vissa förutsättningar, i första hand när sökanden haft hemvist i Sverige i minst tio år. Visserligen kan

risken för att en felaktig eller falsk identitet uppstår i ett ärende om svenskt medborgarskap bedömas som förhållandevis låg, eftersom personen kan antas ha haft kontakt med svenska myndigheter sedan tidigare i ärenden om uppehållstillstånd och folkbokföring. Den identitet som ligger till grund för en ansökan om svenskt medborgarskap har då fastställts i de ärendena. En noggrann kontroll måste dock alltid göras, med hänsyn till att ett beslut om naturalisation i princip är oåterkalleligt[15], vilket så att säga skulle ”cementera” en falsk eller felaktig identitet.

För personer som folkbokförs i samband med födelse i Sverige tillämpas inte något särskilt beviskrav utan i den stora majoriteten av ärenden kan Skatteverket, efter kontroll i folkbokföringen, folkbokföra barnet utifrån uppgifter som lämnats i en anmälan från barnmorska. Vid en anmälan om födelse från vårdnadshavare behöver vårdnadshavarens identitet kontrolleras, liksom de intyg som åberopas för att visa vem som fött barnet. Det bör sällan kunna förekomma felaktiga eller falska uppgifter om identiteten för ett barn som föds i Sverige, eftersom namn och födelsetid kan anses vara kända redan från början. För uppgifter om medborgarskap kan det dock tänkas att felaktiga sådana uppgifter i realiteten ”ärvs” från föräldrarna.

Konsekvenser av falska och felaktiga identiteter

En felaktig eller falsk identitet kan användas för olika syften, i olika sammanhang. Framför allt kan en falsk eller felaktig identitet få betydelse under en persons vistelse i Sverige och vid kontakt med myndigheter och andra aktörer i samhället, men även i förhållande till privatpersoner. Till exempel kan identiteterna användas för att bemanna bolagsstyrelser, som firmatecknare, för att ta lån, för att få bank- och kreditkort, för att använda speltjänster eller för att köpa bilar och andra varor på kredit.

Felaktiga eller falska uppgifter om identiteten kan få betydande konsekvenser redan i samband med att en person vill resa in i Sverige eller påträffas vid en inre utlänningskontroll, utan att han eller hon tidigare varit i kontakt med svenska myndigheter. Korrekt kunskap

[15] I betänkandet *Återkallelse av svenskt medborgarskap*, SOU 2026:21, lämnas förslag som innebär att det svenska medborgarskapet ska kunna fråntas den med dubbla medborgarskap som har förvärvat medborgarskapet genom oriktiga eller ofullständiga uppgifter.

om identiteten är då en förutsättning för att den kontrollerande myndigheten ska kunna kontrollera rätt person. Vid gränskontroller och ansökan om uppehållstillstånd på grund av skyddsbehov ska kontroller göras bland annat mot Schengens informationssystem och Eurodac. Kontrollerna syftar bland annat till att Polismyndigheten eller Migrationsverket ska kunna bedöma vilken medlemsstat som är ansvarig för en ansökan om uppehållstillstånd på grund av behov av internationellt skydd samt få fram uppgifter om hur personen har rest in i Schengenområdet, om personen har ansökt om uppehållstillstånd i något annat land, om personen har utvisats från eller begått brott Sverige eller andra Schengenländer, samt om personen utgör ett säkerhetshot. Dessa kontroller har betydelse dels för det svenska samhället, dels för andra Schengenländer. Om den enskilde åberopar en felaktig eller falsk identitet och de korrekta uppgifterna inte klarläggs riskerar kontroller som genomförs med hjälp av alfanumeriska uppgifter om identiteten i praktiken att bli verkningslösa, och den omständigheten att det finns breda legala möjligheter att vidta kontrollerna blir därmed närmast illusorisk. Möjligheter att identifiera en person eller verifiera hans eller hennes identitet med hjälp av biometriska uppgifter har då en viktig funktion.

Att en felaktig eller falsk identitet etableras i ett ärende kan antas få störst konsekvenser när personen väl vistas i Sverige, i synnerhet när någon lever i landet med en falsk identitet som har skapats medvetet. En falsk eller felaktig identitet kan bland annat användas vid systematiskt utnyttjande av välfärdsförmåner, genom att felaktiga uppgifter om identiteten har registrerats i folkbokföringsverksamheten när en person som har beviljats uppehållstillstånd har folkbokförts i Sverige eller tilldelats ett samordningsnummer av Skatteverket.[16] Migrationsverkets bedömning ligger som utgångspunkt till grund för den identitet som Skatteverket fastställer för personer som beviljats uppehållstillstånd i Sverige.[17] När en uppgift väl har blivit registrerad i folkbokföringsverksamheten finns det begränsade möjligheter att rätta eller korrigera dessa; enligt 22 § folkbokföringslagen (1991:481) ska Skatteverket visserligen avregistrera falska identiteter, men ett sådant beslut förutsätter en noggrann utredning.[18] Ett person- eller samordningsnummer som hänför sig till en falsk identitet kan

[16] *Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra*, SOU 2017:37, s. 267.
[17] RiR 2024:12, s. 5.
[18] Jfr uppgifter om avregistrering av falska identiteter i folkbokföringen i avsnitt 9.2.5.

därför under en längre tid finnas registrerat utan att andra myndigheter får kännedom om att det är en falsk identitet, och identiteten kan under denna tid fortsätta att utnyttjas. Det är alltså av stor vikt att identiteten klarläggs så långt som är möjligt i ärendet hos Migrationsverket. Skatteverket har, i egenskap av ansvarig myndighet för folkbokföringen, beskrivits som en ”grindvakt” för välfärdssystemen.[19]

Samordningsnummer som tilldelats utifrån en falsk eller felaktig identitet kan missbrukas på liknande sätt som beskrivits ovan. Av den kartläggning som gjordes av Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden framgår att flera myndigheter uppmärksammat att falska uppgifter lämnas i syfte att få samordningsnummer, som i sin tur kan leda till utbetalningar från välfärdssystemen, exempelvis i form av lönegaranti där utbetalningar sker till fiktiva anställda som inte existerar. Falska identiteter kan också användas i syfte att dölja vem den verkliga företrädaren i ett bolag är.[20] För den som begår brott genom företag kan användningen av falska identiteter innebära mindre risker och lägre kostnader än att samarbeta med målvakter.[21] Samordningsnummer som har tilldelats utifrån en falsk eller felaktig identitet kan också användas till exempel för att registrera ett stort antal fordon. Det kan bland annat leda till svårigheter med att driva in fordonsrelaterade skatter och avgifter. Det förekommer också att målvaktsfordon används som brottsverktyg.[22]

Felaktiga och falska identiteter utgör också risker inom vården. För det första innebär det en risk att vårda någon som man inte vet vem det är. Det handlar även om att journalen ska föras för rätt patient och om tillgång till korrekt information om patienten (exempelvis blodsmitta, överkänsligheter och tidigare vård).[23]

Ovanstående gör inte anspråk på att vara en uttömmande redogörelse för de konsekvenser som falska eller felaktiga identiteter kan få för samhället. Redovisade exempel visar emellertid, enligt vår mening, tydligt att felaktiga och falska identiteter kan få allvarliga konsekvenser för såväl myndigheter som privata aktörer och enskilda, både i samband med att en person vill resa in i Sverige och under

[19] SOU 2020:35, s. 155.
[20] SOU 2017:37, s. 248 och 296.
[21] *Bolag och brott*, prop. 2024/25:8, s. 38.
[22] *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 30.
[23] Region Stockholm, *ID-kontroll av person som söker vård*, https://vardgivarguiden.se/administration/patientadministration/patientnara-rutiner/id-kontroll/, hämtad den 1 juli 2026.

vistelsen i landet. Utöver detta kan problem uppstå när en person av någon anledning ska utvisas eller avvisas ur landet. Om den identitet som anges i avlägsnandebeslutet visar sig vara oriktig kan identiteten behöva utredas på nytt på verkställighetsstadiet. För att ett avlägsnandebeslut ska kunna verkställas krävs oftast också att utlänningen har eller kan få tillräckliga resehandlingar. Felaktiga eller falska identitetsuppgifter kan då leda till svårigheter att få fram sådana, i syfte att möjliggöra verkställighet av ett avlägsnandebeslut.[24]

9.2.3 Multipla identiteter

Vid multipla identiteter är minst en av identiteterna falsk eller felaktig. Hur dessa i sig kan uppstå och användas har vi redogjort för i föregående avsnitt. I detta avsnitt ger vi exempel på olika sätt som multipla identiteter kan komma att registreras i svenska myndigheters register, i första hand den centrala utlänningsdatabasen och i folkbokföringsverksamheten, och de särskilda konsekvenser de kan medföra.

Vid ansökningar om uppehållstillstånd kan en person skapa flera identiteter på olika sätt. I rapporten *Multipla identiteter inom Migrationsverkets tillstånds- och asylprocess* beskrivs sex huvudsakliga tillvägagångssätt. Den gemensamma nämnaren utgörs av att en ansökan om uppehållstillstånd lämnas in vid en tidpunkt med åberopade av identitet A, och vid ett senare tillfälle lämnas en ny ansökan in varvid identitet B görs gällande.[25] Möjligheten att skapa multipla identiteter vid en ansökan om uppehållstillstånd kan härledas bland annat till de olika beviskrav i fråga om identitet som tillämpas i respektive ärendeslag – i synnerhet det förhållandet att muntliga uppgifter om identiteten kan läggas till grund för identiteten i ärenden om internationellt skydd – och användningen av förfalskade eller manipulerade identitetshandlingar. Som noterats i ovan nämnda rapport från Migrationsverket kan det lägre beviskravet i ärenden om internationellt skydd i praktiken innebära att en svensk medborgare kan ansöka om, och beviljas, detta i Sverige.

När det gäller multipla identiteter hos Skatteverket, det vill säga i folkbokföringsverksamheten, kan dessa uppstå på olika sätt. Eftersom de bedömningar som Migrationsverket gör av identiteten i ären-

[24] *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll*, SOU 2024:80, s. 335.
[25] Migrationsverket, *Multipla identiteter inom Migrationsverkets tillstånds- och asylprocess*, dnr 1.3.4-2024-10939, s. 9 ff.

den om uppehållstillstånd i många fall ligger till grund för senare beslut om folkbokföring utan ytterligare utredning kan multipla identiteter på det sättet få spridning även till folkbokföringen. Ett annat exempel är fall där en person som redan har en identitet registrerad i Sverige ändrar identitetsuppgifter i hemlandet och anmäler flyttning till Sverige under de nya identitetsuppgifterna. Multipla identiteter i folkbokföringsverksamheten behöver dock inte nödvändigtvis bero på ett medvetet eller uppsåtligt agerande utan kan uppstå av misstag. I betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* nämns som exempel att en person, som anmäler flyttning till Sverige, inte är medveten om att han eller hon sedan tidigare har ett person- eller samordningsnummer och att Skatteverket inte upptäcker detta, till exempel på grund av skilda stavningar av namn eller olika angivna födelsedatum.[26]

En kombination av ovanstående situationer kan också tänkas förekomma, vilket innebär att en individ kan vara registrerad med identitet A i den centrala utlänningsdatabasen och med identitet B i folkbokföringsverksamheten. Ett exempel är att en tredjelandsmedborgare felaktigt folkbokförs med uppehållsrätt med hjälp av ett förfalskat pass för EES-medborgare, och att samma person även ansöker om uppehållstillstånd hos Migrationsverket i sin verkliga eller en annan identitet. Om uppehållstillstånd beviljas kan personen komma att folkbokföras under ytterligare en identitet.

Konsekvenser av multipla identiteter

Den brottslighet som möjliggörs genom multipla identiteter kan vara svår att beivra. En person kan leva en form av dubbelliv, där brott begås i den falska identiteten. I en rapport från Brottsförebyggande rådet från år 2016 konstaterades att förutom att detta skapar förutsättningar för omfattande och systematisk brottslighet äventyrar det i förlängningen själva rättssystemet, eftersom det inte är möjligt att veta vem som blivit lagförd.[27]

Med hänsyn till att åtminstone en identitet är falsk eller felaktig när en person är registrerad med multipla identiteter gör sig samma konsekvenser som redogjorts för i föregående avsnitt gällande. An-

[26] SOU 2025:75, s. 410.
[27] Brå, Rapport 2016:9, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag*, s. 162.

vändningen av olika identiteter i olika sammanhang för dock med sig vissa särskilda problem.

I den rapport från Brottsförebyggande rådet som nämnts ovan lyfts bland annat fram att den omständigheten att en person har flera olika identiteter möjliggör för samma person att kombinera arbete och bidrag eller att ansöka om bidrag ur olika system parallellt och på så sätt få ut ersättning felaktigt.[28] I betänkandet *Kommunal anslutning till Utbetalningsmyndighetens verksamhet* noterades att det förekom exempel på att personer med dubbla identiteter får ekonomiskt bistånd från samma kommun i båda identiteterna.[29] Personen kan också ha multipla identiteter i olika EU-länder, för att på så sätt utnyttja flera länders system. På utlänningsrättens område kan multipla identiteter användas exempelvis för att under en ny identitet anmäla inflyttning till Sverige, och på så sätt kringgå ett gällande återreseförbud, vilket kan ha meddelats i samband med en brottmålsdom och utvisning på grund av brott. Som Migrationsverket pekat på i rapporten *Multipla identiteter inom Migrationsverkets tillstånds- och asylprocess* kan multipla identiteter användas av en utlänning för att skaffa svenskt medborgarskap på falska grunder.[30]

En individ som lever i Sverige under ett antal falska identiteter kan använda en eller flera av dem för att begå olika typer av brott. En person med tre olika identiteter skulle exempelvis kunna använda en av dem för att starta ett företag och få startbidrag, den andra för att utge sig för att vara arbetslös och få arbetslöshetsersättning och den tredje för att ta lån som aldrig betalas tillbaka. I ett medialt uppmärksammat fall från år 2020 konstaterades att en kvinna som utfört ett antal stölder i Sverige och andra europeiska länder förekom under minst 15 olika identiteter.[31] Även om en person lagförs för brott i någon av identiteterna kvarstår en risk för att han eller hon i andra sammanhang uppträder under en annan identitet, vilket innebär att den tidigare brottsligheten inte upptäcks, exempel vid kontroll av vandelsvillkoret i ett ärende om svenskt medborgarskap eller när en arbetsgivare gör en kontroll mot misstanke- och belastningsregistret i samband med en eventuell anställning. Konsekvenserna av att en

[28] A.a, s. 118.
[29] SOU 2025:20, s. 98.
[30] Migrationsverket, *Multipla identiteter inom Migrationsverkets tillstånds- och asylprocess*, s. 6.
[31] *Tre personer – 38 identiteter: "Ett stort samhällsproblem"*, https://www.svt.se/nyheter/inrikes/tre-personer-38-identiteter-ett-stort-samhallsproblem, hämtad den 1 juli 2026.

person kan ha multipla identiteter drabbar alltså inte endast myndigheter utan även privata aktörer och enskilda personer.

9.2.4 Utnyttjande av identiteter

Vi har i avsnitt 9.2.2 och 9.2.3 gett flera exempel på hur felaktiga eller falska identiteter kan användas. Inte bara felaktiga och falska identiteter utnyttjas, utan ett allt större problem är att helt korrekta identiteter används av andra personer i olika syften. Som vi noterat i avsnitt 9.2.1 är detta kriminaliserat genom bestämmelsen om olovlig identitetsanvändning i 4 kap. 6 b § brottsbalken. Utnyttjade identiteter sker både på så sätt att personen vars identitet utnyttjas vet om det eller är helt omedveten. Förutom rena kapningar eller stölder av andras identiteter är det inte ovanligt att en person frivilligt, alternativt under hot, lånar ut sina identitetsuppgifter och på så sätt fungerar som en så kallad målvakt.

I en rapport från Skatteverket som vi har tagit del av lyfts bland annat fram att när man fokuserar på ekonomisk brottslighet framstår det med betydande tydlighet som att identitetsrelaterade problem i Sverige är mer kopplade till utnyttjade identiteter än till falska identiteter, även om båda kan förekomma. En orsak kan tänkas vara att det är enklare att utnyttja en korrekt utfärdad identitet än att skapa en falsk identitet. Av rapport från Polismyndigheten framgår att utnyttjade identiteter har upptäckts vara en avgörande del i avancerade penningtvättsupplägg.[32]

Ett upplägg där personer – exempelvis EES-medborgare som kan utnyttja rätten till fri rörlighet inom unionen – hämtas till Sverige i syfte att få ett person- eller samordningsnummer kan användas på många olika sätt. Det förekommer även att identiteten för en person som tidigare har vistats lagligen i Sverige, men lämnat landet utan att avregistrera sig från folkbokföringen, används. Den utresta personens identitet kan därmed användas, med eller utan hans eller hennes vetskap.

Genom folkbokföringen öppnas i praktiken många vägar till bosättningsbaserade förmåner och tillgång till utfärdande av en identitetshandling och en e-legitimation. Identiteten och handlingarna kan

[32] Polismyndighetens rapport, *Systematisk penningtvätt inom den rysktalande organiserade brottsligheten*, dnr A629.012/2024.

därefter utnyttjas för att registrera köp av fastigheter och fordon på personen och för att registrera familjerelationer, som kan ligga till grund för senare ansökningar om uppehållstillstånd. Vid brottslighet som sker genom företag är det också vanligt att målvakter anmäls som företrädare för företaget. Personen är alltså legal företrädare men har inte för avsikt att delta i verksamheten. Syftet med att registrera målvakter är att dölja de personer som i själva verket kontrollerar företaget och som kan använda det för att begå brott. De faktiska företrädarna, som inte syns i Bolagsverkets register, blir på detta sätt svårare att identifiera för de brottsbekämpande myndigheterna och kan undkomma ansvar. Ofta är det medborgare från ett annat EU-land som folkbokförs i Sverige och placeras i styrelsen på ett kreditvärdigt bolag, som sedan genomför omfattande kreditköp innan det försätts i konkurs. För att motverka den typen av upplägg har Bolagsverket från den 1 januari 2025 fått möjlighet att kräva personlig inställelse i vissa fall. I förarbetena konstaterades bland annat att det har blivit vanligare med så kallade utnyttjade identiteter, exempelvis genom att personer från andra länder erbjuds en summa pengar för att ta sig till Sverige och etablera en identitet här. Personen bakom identiteten kan sedan lämna landet och överlåta identiteten till andra. Även dessa utnyttjade identiteter ansågs vara ett slags målvakter.[33]

Utnyttjande av identiteter främjas av att kontakterna mellan personer och myndigheter i allt större utsträckning sker på digital väg. När det gäller socialförsäkringsförmåner som handläggs av Försäkringskassan och Pensionsmyndigheten gör dessa myndigheter i nuläget begränsade, eller inga, kontroller för att säkerställa att en person som ansöker om en förmån hör ihop med det personnummer som används; vid kontroll av identiteten förlitar sig dessa myndigheter på användning av e-legitimation och de säkerhetskrav som utfärdaren av e-legitimationen föreskriver. Eftersom användningen sker på distans behöver den person som e-legitimationen tillhör inte befinna sig i Sverige, vilket ytterligare minskar exponeringen. Vid behov hämtas personen till Sverige och ställer upp vid en eventuell identitetskontroll.[34]

Att förhindra utnyttjande av identiteter tar sikte på verifiering av en redan etablerad identitet, medan åtgärder för att motverka att

[33] Prop. 2024/25:8, s. 38.
[34] SOU 2023:61, s. 117.

felaktiga eller falska identiteter uppstår i första hand genomförs i samband med det ärende där en identitet för första gången registreras hos svenska myndigheter. I Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* framgår bland annat att flera experter lyft fram att den största risken för identitetsrelaterade välfärdsbrott finns just vid själva verifieringen av identitet, genom att personen som använder e-legitimationen inte hör ihop med personen som han eller hon utger sig för att vara. Orsaken anges vara att det är enklare att utnyttja en korrekt utfärdad identitet än att skapa en falsk identitet. Detta beror inte minst på att digitaliseringen har förenklat att identiteter missbrukas på distans i brottsligt syfte.[35]

9.2.5 Omfattningen av identitetsmissbruk

Vår bedömning

Omfattningen av identitetsmissbruk är svår att bedöma. Det finns dock anledning att anta att det finns ett stort mörkertal, att missbruket riktas mot en större krets samhällsaktörer och att omfattningen är på en sådan nivå att ytterligare åtgärder bör övervägas.

Som framgår av kartläggningen i kapitel 7, och som vi återkommer till i kapitel 10, har Skatteverket, Migrationsverket och Polismyndigheten ett relativt brett författningsstöd, både gällande och föreslaget, som syftar till att motverka att felaktiga, falska och multipla identiteter uppstår.

Vi kan konstatera att det generellt sett är mycket svårt att tillförlitligt uppskatta i vilken utsträckning identitetsmissbruk som har en koppling till falska, felaktiga, multipla eller utnyttjade identiteter förekommer. Det beror bland annat på att det kan antas finnas ett stort mörkertal, på grund av att det helt enkelt är svårt eller omöjligt att i många fall veta om en viss identitet är falsk eller utnyttjad. En inkonsekvent användning av olika identitetsbegrepp och det faktum att en person kan förekomma under flera olika identiteter, inte bara i en utan i olika myndigheters register, bidrar till svårigheten att göra en samlad uppskattning av omfattningen av fel – bland annat i folk-

[35] RiR 2024:12, s. 68.

bokföringsverksamheten – som är hänförliga till felaktiga eller falska identiteter.[36]

Enligt vår bedömning finns det emellertid anledning att anta att identitetsmissbruk är vanligt förekommande. Brottsförebyggande rådet framhöll i en rapport redan från år 2016 att det fanns indikationer på att användningen av stulna och falska identiteter ökar i Sverige; bruket av helt falska identiteter utan några kopplingar till existerande personer utgjorde, enligt de aktörer som Brottsförebyggande rådet intervjuade, ett omfattande och inte speciellt uppmärksammat problem.[37] I rapport från Skatteverket från år 2022, *Sammanhållen identitetsförvaltning*, anfördes bland annat att antalet brott kopplade till användande av identitetsuppgifter har ökat kraftigt de senaste åren, och Utredningen om brottsbekämpning inom Skatteverket gjorde i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* bedömningen att det får anses stå klart att folkbokföringsfel med koppling till identitet är ett omfattande problem som rör flera myndigheter.[38] En sådan bedömning får enligt vår mening även stöd i den kartläggning som gjordes av Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden, som visade på att det förekom anmälningar om bidragsbrott där falska eller felaktiga identiteter hade använts i ärenden om etableringsersättning och nystartsjobb, att oriktig identitet hade upptäckts i 25 procent av anmälningarna som riktas mot Arbetsförmedlingen, att multipla identiteter hade använts i ärenden om både arbetslöshetsersättning och aktivitetsstöd och att utnyttjande av identitet hade uppmärksammats hos kommunerna, även om det rörde sig om något enstaka fall. Det lyftes även fram att flera myndigheter hade uppmärksammat att falska identitetsuppgifter lämnas i syfte att få samordningsnummer, som i sin tur kan leda till utbetalningar från välfärdssystemen.[39]

En uppskattning av storleken på felaktigt utbetalda belopp kan också ge en fingervisning om omfattningen; enligt Riksrevisionens sammanställning uppgick omfattningen av de förmåner som betalats ut till EES-medborgare till närmare 115 miljarder kronor för åren 2011–2021. Även om endast en mindre andel av dessa utbetalningar skulle ske på felaktig grund kopplat till identitetsmissbruk kan det,

[36] SOU 2025:75, s. 410.
[37] Brå, Rapport 2016:9, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag*, s. 148 f.
[38] SOU 2025:75, s. 414.
[39] SOU 2017:37, s. 203, 206, 210, 221, 238 och 248.

enligt Riksrevisionen, antas röra sig om mycket betydande belopp.[40] Vi delar denna bedömning.

En indikation på omfattningen av falska identiteter i folkbokföringsverksamheten är hur många sådana som har avregistrerats av Skatteverket med stöd av 22 § folkbokföringslagen; från att bestämmelsen infördes år 2018 till och med april 2025 beslutade myndigheten om avregistrering i 397 ärenden, varav 396 avsåg identiteter med registrerat medborgarskap inom EU eller EES. Med hänsyn till svårigheten i att upptäcka falska identiteter är det, enligt vår bedömning, rimligt att anta att det finns ett betydande mörkertal.

När det gäller dubbla samordningsnummer uppskattade Utredningen om brottsbekämpning inom Skatteverket att det förekommer cirka 11 000 sådana. I samma utredning uppgav Migrationsverket att det är mycket svårt att uppskatta omfattningen av falska och felaktiga samt multipla identiteter i myndighetens verksamhet, men att av samtliga ansiktsjämförelser som myndigheten gjorde efter tips från verksamheten år 2023 upptäcktes alias i knappt 20 procent av fallen. Enligt myndigheten var bilden dock troligen inte representativ.[41] Som jämförelse framgår av Migrationsverkets rapport om multipla identiteter från år 2024 att vid granskning av 102 slumpmässigt utvalda ärenden identifierades multipla identiteter i 15 av dem, det vill säga motsvarande cirka 15 procent.[42] Värt att notera är även att i interpellation 2021/22:166, *Utlänningars identitet*, gjordes gällande att Migrationsverket år 2017 gjort bedömningen att det fanns nära 60 000 individer registrerade med två eller flera kända identiteter hos myndigheten och att verket konstaterade att mörkertalet var stort.

Som nämnts ovan har Skatteverket bedömt att identitetsrelaterade problem i Sverige är mer kopplade till utnyttjade identiteter än till falska identiteter. Sedan år 2016 är olaglig identitetsanvändning kriminaliserat. Antalet sådana anmälda brott framgår av statistik från Brottsförebyggande rådet, enligt tabellen nedan.

Tabell 9.1 Anmälda fall av olovlig identitetsanvändning

2019	2020	2021	2022	2023	2024	2025
29 255	31 427	26 499	19 329	16 833	17 759	15 413

[40] RiR 2024:12, s. 9.
[41] SOU 2025:75, s. 412 och 414.
[42] Migrationsverket, *Multipla identiteter inom Migrationsverkets tillstånds- och asylprocess*, s. 9.

Sammanfattningsvis kan vi konstatera att det synes vara svårt att få en klar bild av den faktiska omfattningen av identitetsmissbruk inom olika områden. Oaktat detta delar vi den bedömning som gjordes av Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden, att redan det faktum att oriktiga identiteter förekommer, vilket kan skapa möjligheter att begå brott mot välfärdssystemen, gör förekomsten särskilt angelägen att motverka.[43] Tidigare utredningar och statistik visar enligt vår mening också på att felaktiga, falska och multipla identiteter och utnyttjande av identiteter förekommer inom flera sektorer och att detta påverkar samhället negativt, men även privatpersoner. Utöver att identitetsmissbruk kan leda till att förmåner utgår på fel grunder till fel personer möjliggör det avancerade brottsliga upplägg. I längden påverkas tilliten till identitetsförvaltningen, både hos myndigheter och enskilda personer. Att motverka identitetsmissbruk och främja en säker verifiering av identitet är, som lyfts fram av experter under utredningen, inte bara viktigt ur en kontrollsynpunkt utan även som en trygghet för enskilda.

Även om det inte är möjligt att närmare uppskatta omfattningen av identitetsmissbruk anser vi att de mätpunkter som redogjorts för ovan talar för att felaktiga, falska, multipla och utnyttjade identiteter förekommer på en sådan nivå att det motiverar att vidare åtgärder övervägs, särskilt med beaktande av att det kan antas finnas ett stort mörkertal. Att identitetsmissbruket riktas mot och får följder för många myndigheter och centrala samhällsfunktioner talar ytterligare för en sådan bedömning.

[43] SOU 2017:37, s. 267.

10 Tänkbara åtgärder för säkrare verifiering av identitet

10.1 Inledning

I föregående kapitel har vi beskrivit hur felaktiga, falska och multipla identiteter kan uppkomma och registreras i olika situationer och hur identiteter kan utnyttjas. Frågan är vilka åtgärder som på ett effektivt sätt kan antas kunna motverka detta. Vårt övergripande uppdrag är, enligt direktiven, att lämna förslag som stärker kopplingen till den identitet som etableras av Polismyndigheten, Migrationsverket eller Skatteverket i olika ärenden, vid verifiering av identitet med hjälp av biometriska uppgifter. Fokus för vårt uppdrag är alltså dels *verifiering* av redan etablerade identiteter, dels att verifieringen ska ha sin grund i *biometriska uppgifter*. Vidare tar direktiven sikte på ett system för säkrare verifiering av identitet – genom just stärkt koppling mellan etablerad identitet och verifiering av identitet med hjälp av biometriska uppgifter – och framhåller behovet av en sammanhållen identitetsförvaltning och av att fler aktörer än i dag kan få ta del av information om en etablerad identitet för att förstärka sin kontroll i verifieringssteget. Vårt uppdrag går alltså – som utgångspunkt – inte ut på att utvärdera och förbättra gällande regelverk.

Våra överväganden i detta kapitel tar i första hand sikte på åtgärder som kan främja vårt uppdrag. Det är enligt vår mening emellertid också viktigt att eftersträva att korrekta identitetsuppgifter registreras när en identitet etableras. Vi kommer därför även att ta ställning till vissa åtgärder som kan stärka Polismyndighetens, Migrationsverkets och Skatteverkets arbete med att etablera en identitet. Inledningsvis behandlar vi också åtgärder av generell karaktär som kan få betydelse såväl vid etablering av en identitet som vid verifiering av identitet i ett senare skede.

10.2 Åtgärder av generell karaktär

Vi anser att det inledningsvis finns anledning att belysa vissa åtgärder som inte är knutna till just verifiering av identitet men som kan få betydelse för att stärka dels arbetet med att etablera en grundidentitet, dels kopplingen mellan en sådan identitet och verifiering av denna med hjälp av biometriska uppgifter, i vart fall indirekt.

10.2.1 Kompetenshöjande åtgärder och metodutveckling

Vår bedömning

Åtgärder för att öka myndigheters kompetens och utveckla metoderna för att etablera en korrekt grundidentitet bör vidtas i annan ordning än genom lagstiftning.

I Riksrevisions rapport *Vem där – fastställande av identitet vid statliga myndigheter* identifierades ett flertal brister i fråga om myndigheternas tillgång till kompetens för att säkerställa att de fastställer identitet korrekt, och det påpekades att de stödfunktioner som finns är underutnyttjade. Det konstaterades också att de granskade myndigheternas processer inte bidrar tillräckligt till att korrekta och unika identiteter etableras, och att det finns ett behov av ökat informationsutbyte hos samtliga myndigheter för att förbättra fastställande av korrekta identiteter.[1] Brister av nämnda slag kan enligt vår bedömning inte åtgärdas genom lagstiftningsåtgärder utan genom åtgärder på myndighetsnivå. Regeringen har som en följd av Riksrevisionens rapport lämnat uppdrag till de kontrollerande myndigheterna samt Statens servicecenter att stärka samarbetet för att upprätthålla och sprida kompetens om identitetsfrågor (Fi2024/02215), och att utveckla det operativa samarbetet för att motverka identitetsmissbruk (Fi2024/02214). Redovisningar med förslag på åtgärder har lämnats av Skatteverket.[2] Vi kan även notera att Migrationsverket den 26 september 2024 överlämnade rapporten *Åtgärder för att stärka kontrollerna i ärenden gällande medborgarskap.* Av rapporten framgår bland annat att myndigheten avser att ta fram en gemensam standard för ett gemensamt

[1] RiR 2024:12, s. 97.
[2] Skatteverkets del- respektive slutredovisningar från den 31 mars respektive den 13 juni 2025, dnr 8-93999-2025 och 8-154768-2025.

arbets- och granskningssätt i dessa ärenden, och att myndigheten identifierat ett behov av en översyn av vilka handlingar som skickas vidare till id-enheterna för mer omfattande granskning samt ett behov av att handläggande personal med granskningskompetens ska ges ytterligare utbildning, gällande till exempel fotojämförelser.

Ovan nämnda uppdrag kan enligt vår bedömning antas bidra till att motverka de brister i Polismyndighetens, Migrationsverkets och Skatteverkets arbete med att etablera en korrekt identitet som pekades på i Riksrevisionens rapport. Om ytterligare behov av att öka kompetensen och samarbetet mellan dessa myndigheter identifieras bör det tas om hand på annat sätt än genom lagstiftningsåtgärder. Vi utvärderar därför inte några kompetenshöjande åtgärder eller metoder för att utveckla dessa myndigheters befintliga arbete.

10.2.2 Högre beviskrav i fråga om identitet

Vår bedömning

Det är inte möjligt att, inom ramen för vårt uppdrag, generellt införa ett visst beviskrav i fråga om identitet för att främja en stärkt koppling mellan etablerad identitet och verifiering av identitet.

En bidragande faktor till att oriktiga identiteter kan registreras är, som vi pekat på i avsnitt 9.2.2, att olika beviskrav kan tillämpas i olika ärendeslag. När det gäller att lägre beviskrav än styrkt kan medföra att även en person med en oklar identitet beviljas uppehållstillstånd och sedan folkbokförs i Sverige skulle ett genomgående krav på styrkt identitet visserligen kunna motverka falska eller felaktiga identiteter. Möjligheten att skapa multipla identiteter kan också i viss mån härledas till de olika beviskrav i fråga om identitet som tillämpas i olika ärendeslag som Migrationsverket handlägger – inte minst det förhållandet att muntliga uppgifter om identiteten kan läggas till grund för den identitet som registreras i ärenden om uppehållstillstånd på grund av behov av internationellt skydd. Vi kan emellertid konstatera att det i sistnämnda ärendeslag inte alls är möjligt att tillämpa ett sådant beviskrav, med hänsyn till Sveriges internationella förpliktelser och praxis. Vidare saknas det i många andra ärendeslag beviskrav avseende identitet. Som exempel kan nämnas ärenden om socialförsäkringsförmåner

som handläggs av Försäkringskassan. Socialförsäkringsbalken innehåller inte några bestämmelser som anger med vilken styrka den som ansöker om en förmån ska visa vem han eller hon är. Överväganden om att införa en helt ny ordning i fråga om beviskrav i socialförsäkringsbalken skulle enligt vår uppfattning inte vara möjligt, eller lämpligt, att göra, i vart fall inte inom ramen för detta betänkande. En ändring i beviskravet avseende identitet i olika ärendeslag skulle kräva en översyn av ett mycket stort antal författningar.

Det är mot denna bakgrund oklart om det alls är möjligt att införa ett visst, högre, beviskrav i många av de ärenden där identitet kan behöva verifieras. Under alla omständigheter kan en sådan mer övergripande översyn inte anses ingå i vårt uppdrag. Att identiteten kan anses styrkt innebär inte heller att den också alltid kan anses verifierad; dessa frågor är – som vi redogjort för i avsnitt 7.2.2 – inte beroende av varandra.

10.2.3 Utökade möjligheter att kräva personlig inställelse

Vår bedömning

Utökade möjligheter för myndigheter att kräva personlig inställelse kan stärka kopplingen mellan en etablerad identitet och verifiering av identitet och vara en viktig komponent i att kunna genomföra verifiering med hjälp av biometriska uppgifter.

Digitaliseringen i samhället har på många sätt öppnat upp för smidiga ansökningsprocesser och kontakter med myndigheter. I många ärendeslag görs ansökan regelmässigt på distans. I Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* konstaterades bland annat att verifiering av identitet, i ärenden där Försäkringskassan ska pröva och utbetala förmåner till personer som redan finns inlagda i myndighetens system, normalt sker genom att personen legitimerar sig genom någon form av e-legitimation.[3] Det får enligt vår mening antas höra till undantagen att enskilda ansöker om förmåner av mer återkommande slag, exempelvis sjukpenning eller tillfällig föräldrapenning, vid ett besök på plats hos myndigheten. En tydlig nackdel med en ökad digitalisering är emellertid att använd-

[3] RiR 2024:12, s. 68.

ning av exempelvis falska identiteter underlättas av att det inte sker en verifiering vid ett fysiskt möte. I förarbetena till den möjlighet för Bolagsverket att förelägga någon att inställa sig personligen som införts i 27 kap. 2 § aktiebolagslagen (2005:551) anfördes bland annat att en säkrare bedömning av identiteten kan göras vid personlig inställelse, genom att en jämförelse mellan personen och dennes identitetshandlingar kan göras. Vidare kan det ställas kontrollfrågor. Ett föreläggande om personlig inställelse bedömdes också kunna ha en preventiv verkan.[4]

Personlig inställelse används regelmässigt i de ärendeslag som beskrivits i kapitel 6. Vissa av dessa – exempelvis en gränskontroll eller en inre utlänningskontroll – är till sin natur sådana att den enskilde närvarar på plats. Även vid en ansökan om uppehållstillstånd är sökanden normalt närvarande åtminstone vid någon tidpunkt under utredningen av hans eller hennes ansökan. I ärendeslag som inte naturligen kräver personlig närvaro har uttryckligt stöd för detta införts i vissa fall. Ett exempel är 26 a § folkbokföringslagen (1991:481), som anger att den som enligt 26 § ska lämna en anmälan om flyttning från utlandet *ska* inställa sig personligen hos Skatteverket för identitetskontroll. Vid en ansökan om pass anges i 6 § passlagen (1978:302) att sökanden är skyldig att inställa sig personligen. I samband med detta är sökanden även skyldig att låta Polismyndigheten ta hans eller hennes fingeravtryck och en ansiktsbild i digitalt format.

Vi delar bedömningen att personlig inställelse kan vara av betydelse för en säkrare identitetskontroll och att det ger bättre förutsättningar att koppla en fysisk person till de identitetsuppgifter som finns i en ansökan, anmälan eller en identitetshandling som han eller hon använder för att legitimera sig; även en okulär kontroll mot ett fotografi i en identitetshandling kräver personlig inställelse. Nu tillgängliga och tillämpade tekniska lösningar innebär att personlig inställelse närmast är en förutsättning för att biometriska underlag ska kunna tas upp, och därmed också för att kunna stärka kopplingen mellan en etablerad identitet och verifiering av identitet med hjälp av biometriska uppgifter som kan tas fram ur underlagen, oavsett om jämförelsen görs mot ett register eller mot en identitetshandling. För att en säkrare verifiering av identitet med hjälp av biometriska uppgifter ska kunna få ett faktiskt genomslag och inte endast bli en pappersprodukt anser vi, som vi återkommer till i kapitel 27, dock

[4] *Bolag och brott*, prop. 2024/25:8, s. 41.

att utgångspunkten bör vara att en verifiering ska kunna genomföras såväl vid personlig inställelse som på distans. Vidare bedömer vi, i avsnitt 18.3.2 och 20.3, utifrån liknande resonemang att det inte bör regleras i författning hur biometriska underlag tas upp vid verifiering av identitet med hjälp av biometriska uppgifter som kan tas fram ur underlagen. Att det inte bör regleras att upptagningen av biometriska underlag alltid ska ske vid personlig inställelse utesluter emellertid inte att det inte kan övervägas om myndigheter bör ges en utökad möjlighet att, som *ett led i* att kunna biometriskt verifiera identitet, kräva att den vars identitet ska kontrolleras inställer sig personligen. Detta kan också följa indirekt av ett krav på att göra en handling tillgänglig i syfte att genomföra en biometrisk verifiering av identitet, beroende på hur verifieringen kan komma att genomföras tekniskt. Vi återkommer till detta i avsnitt 23.6.4.

10.3 Åtgärder när en identitet behöver etableras

Som framgår av kapitel 7 och 8 har det inom EU och nationellt vidtagits ett stort antal lagstiftningsåtgärder under senare år som bland annat syftar till en bättre kontroll av individer som vill resa in i och vistas i Sverige, däribland genom att öka möjligheterna för myndigheterna att använda biometriska uppgifter för att uppnå dessa syften. Det är sammantaget fråga om en bred flora bestämmelser och effekten av dem är svår att utvärdera i nuläget. Frågan är ändå om nuvarande och föreslaget stöd för att använda biometriska uppgifter är tillräckligt för att motverka att felaktiga, falska och multipla identiteter etableras, vilket vi utvärderar i det här avsnittet. Avsnittet fokuserar på de ärenden som redogjorts för i kapitel 6 och som handläggs av Polismyndigheten, Migrationsverket och Skatteverket.

10.3.1 Utökad användning av biometriska uppgifter

Vår bedömning

Det finns ett brett rättsligt stöd för Polismyndigheten, Migrationsverket och Skatteverket att använda biometriska uppgifter för att kunna etablera en identitet i de ärendeslag som vi har beskrivit i kapitel 6. Det bör därför inte övervägas att, inom ramen för denna utredning, lämna förslag som tar sikte på befintliga regelverk i dessa avseenden.

Att kunna använda biometriska uppgifter för att verifiera identiteten och – om så är nödvändigt – identifiera en person utgör en betydelsefull komponent i att motverka identitetsmissbruk och främja att korrekta identiteter etableras. Detta har lyfts fram i flera sammanhang: bland annat anförde Skatteverket i en hemställan till regeringen att det förutsätts att biometriska uppgifter används och kan kopplas till en individ för att ett mål om ”en person, en identitet” ska kunna uppnås.[5] Genom att jämföra biometriska uppgifter, som tagits fram ur de biometriska underlag som tagits upp av personen i fråga, med sådana som sedan tidigare är lagrade i ett register främjas möjligheten att etablera en korrekt identitet även när det saknas krav på att identiteten ska styrkas med en godtagbar identitetshandling. Det är också en viktig del i att kunna följa en viss individ över tid, oavsett om han eller hon försöker använda olika identitetsuppgifter vid olika tillfällen. Att kunna identifiera någon med hjälp av biometriska uppgifter – och på det sättet verifiera identitet – fyller också detta syfte, och är dessutom ett effektivt sätt både att förhindra att multipla identiteter registreras och att motverka att identitetskontroller är begränsade till ett ”stuprör”, det vill säga att de görs endast inom ett visst ärende eller av en viss myndighet. Vidare säkerställer en jämförelse av biometriska uppgifter i en identitetshandling med de biometriska underlag som kan tas upp av den enskilde att handlingen är utfärdad till den person som myndigheten möter, även om underlaget för identitetshandlingen i sig kan vara felaktigt.

[5] *Behov av en sammanhållen infrastruktur för identitet*, Skatteverket, dnr 8/2765903, 2024-01-19.

Det finns ett brett stöd för att använda biometriska uppgifter

Av kartläggningen i kapitel 7 framgår, vilket vi återkommer till nedan, enligt vår mening att det sammantaget finns ett brett gällande, beslutat och föreslaget rättsligt stöd för Polismyndigheten, Migrationsverket och Skatteverket att, i ärendeslag där en identitet kan behöva etableras, ta upp biometriska underlag och använda de biometriska uppgifter som kan tas fram ur dessa för att verifiera identitet genom att jämföra dessa med uppgifter som kan finnas lagrade i identitetshandlingar eller i befintliga nationella register och EU-gemensamma informationssystem. Detsamma gäller för möjligheten att identifiera personer, när identiteten inte kan verifieras. Som framgår av kartläggningen kan Polismyndigheten och Migrationsverket använda biometriska uppgifter i olika sammanhang, bland annat vid ansökan om uppehållstillstånd och medborgarskap, vid yttre gränskontroller och vid inre utlänningskontroller. De biometriska underlag som tas upp av nämnda myndigheter får i vissa ärendeslag också lagras i Migrationsverkets register över fingeravtryck och fotografier med stöd av 15 § utlänningsdatalagen (2016:27). Vidare kan Skatteverket i ärenden om folkbokföring och samordningsnummer ta upp biometriska underlag i samband med en identitetskontroll för att jämföra de biometriska uppgifter som tas fram ur dem mot biometriska underlag som finns lagrade i en identitetshandling. Flera förslag om utökade möjligheter för dessa myndigheter att använda och lagra biometriska uppgifter har också lämnats, där följande särskilt kan nämnas.

I propositionen *Stärkt återvändandeverksamhet* har förslag lämnats om att biometriska underlag som tas upp i samband med alla ansökningar om uppehållstillstånd – och inte bara som nu vid ansökan om internationellt skydd – ska få lagras i Migrationsverkets register.[6] Vidare har det föreslagits att biometriska underlag ska få tas upp om det behövs i ett ärende om avvisning eller utvisning och att en ny bestämmelse ska införas i 13 f § lagen (2001:82) om svenskt medborgarskap, som syftar till att ge Migrationsverket möjlighet att ta upp biometriska underlag även i ärenden om anmälan eller ansökan om svenskt medborgarskap, för att kunna kontrollera dessa mot uppgifter som finns lagrade i utlänningens uppehållstillståndskort eller i Migrationsverkets register över fingeravtryck och fotografier.[7] De

[6] Prop. 2025/26:263, s. 123 f. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.
[7] Prop. 2025/26:263, s. 126 och 129 f.

biometriska underlag som tas upp i nämnda ärendeslag ska under vissa förutsättningar också kunna lagras i sistnämnda register.

Polismyndigheten föreslås också få större möjlighet att med hjälp av biometriska uppgifter söka i fler EU-gemensamma system. I departementspromemorian *Anpassningar av svensk rätt till EU:s förordningar om interoperabilitet* lämnades förslag om att en ny bestämmelse i 9 kap. 8 j § utlänningslagen (2005:716) ska införas, som ger myndigheten rätt att vid en inre utlänningskontroll ta upp biometriska underlag av en utlänning för att söka i EU:s gemensamma databas för identitetsuppgifter, CIR.[8] CIR har tagits i drift den 12 juni 2026.[9] Utöver detta har förslag lämnats i propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* som innebär utökade möjligheter för Skatteverket att efter att ett ärende avslutats lagra biometriska underlag och biometriska uppgifter som har tagits fram vid en identitetskontroll, och att använda dem för en automatiserad jämförelse också med uppgifter som finnas lagrade hos Migrationsverket. Sistnämnda myndighet föreslogs samtidigt få en motsvarande möjlighet att jämföra biometriska uppgifter med uppgifter som finns lagrade hos Skatteverket.[10] Vi kan i detta sammanhang även notera att enligt förslag i betänkandet *Registrering av EES-medborgare* ska ett särskilt, obligatoriskt, registreringsförfarande för EES-medborgare som vistas i Sverige i mer än tre månader återinföras. I betänkandet föreslogs bland annat att Migrationsverket ska få fotografera en EES-medborgare och ta hans eller hennes fingeravtryck i samband med ansökan om registrering av uppehållsrätt, i syfte att verifiera sökandens identitet.[11]

Att delar av det rättsliga stödet för Polismyndigheten, Migrationsverket och Skatteverket att i större omfattning än i dag använda biometriska uppgifter ännu inte har beslutats eller trätt i kraft innebär att det kan vara svårt att utvärdera effekten i praktiken. Att möjligheten att lagra biometriska uppgifter i fler ärendeslag utgörs av förslag innebär också att befintliga register inte innehåller sådana uppgifter i nuläget, utan kommer att byggas upp efterhand. Nämnda begränsningar innebär enligt vår mening emellertid inte att det i sig saknas ett rättsligt stöd för nämnda myndigheter att använda biometriska

[8] Ds 2022:21, s. 89.
[9] Se artikel 1 i Kommissionens genomförandebeslut (EU) 2026/1156 av den 28 maj 2026.
[10] Prop. 2025/26:261, s. 101, 103 f. och 109.
[11] SOU 2026:9, s. 119.

uppgifter för att verifiera identitet eller identifiera en person. Vissa andra begränsningar kan dock urskiljas, vilket vi redogör för nedan.

Vissa begränsningar hänförliga till ålder

Kretsen av personer som omfattas av bestämmelser som medför en skyldighet att lämna biometriska underlag i olika situationer är till viss del begränsad med hänsyn till ålder. Enligt gällande lydelse kan fingeravtryck tas med stöd av 9 kap. 8 § utlänningslagen endast om personen har fyllt 14 år. I syfte att motverka att barn blir utsatta för människohandel och exploatering och för att bättre harmonisera med EU-förordningar på migrationsområdet har det emellertid lämnats förslag i propositionen *Utmönstring av permanent uppehållstillstånd och anpassning av svensk rätt till EU:s migrations- och asylpakt* om att åldersgränsen ska sänkas till sex år. Regleringen innebär inte en skyldighet att ta fingeravtryck från alla barn som har fyllt sex år utan fingeravtryck bör tas i situationer där det finns behov av det. En bedömning ska enligt förslagen göras i det enskilda fallet, med beaktande av barnets bästa.[12] I 9 kap. 8 d § utlänningslagen anges en gräns om tolv år för att ta fingeravtryck för att söka i in- och utresesystemet vid en gränskontroll. Detta följer direkt av artikel 17.3 i in- och utreseförordningen[13]. En lägre åldersgräns kan därför inte tillämpas i nationell rätt.

I ärenden om folkbokföring och samordningsnummer saknas, enligt 26 a § folkbokföringslagen och 2 kap. 4 § lagen (2022:1697) om samordningsnummer, en nedre åldersgräns för att ta upp ansiktsbilder. En åldersgräns på 14 år har dock föreslagits beträffande Skatteverkets möjligheter att få göra automatiserade jämförelser med hjälp av biometriska uppgifter mot Migrationsverkets register. Detta register innehåller i dagsläget endast uppgifter om personer som har fyllt 14 år. Trots att den nedre åldersgränsen enligt förslag ska ändras till sex år (se ovan) har regeringen bedömt att det inte kommit fram behov för Skatteverket att göra biometriska jämförelser med uppgifter som finns i Migrationsverkets register för barn under 14 år.[14]

[12] Prop. 2025/26:262, s. 45 och 417 f.
[13] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.
[14] Prop. 2025/26:261, s. 81 och 103 f.

Begränsningar hänförliga till medborgarskap

Kretsen av personer som kan vara skyldiga att lämna biometriska underlag i de ärendeslag som vi beskrivit i kapitel 6 avgränsas inte bara genom ålder. För det första är möjligheterna att använda biometriska uppgifter för att söka i EU-gemensamma informationssystem begränsade till tredjelandsmedborgare. Till exempel framgår av artikel 2 i in- och utreseförordningen att förordningen endast är tillämplig på tredjelandsmedborgare. Personer som omfattas av rörlighetsdirektivet[15] omfattas enligt artikel 2.3 inte och det är endast uppgifter om tredjelandsmedborgare som registreras i systemet. Sökningar för att verifiera identiteten eller identifiera en person enligt artikel 26 och 27 är begränsade till att avse tredjelandsmedborgare. De kompletterande bestämmelser som finns i 9 kap. utlänningslagen som ger Polismyndigheten och Migrationsverket rätt att ta upp biometriska underlag i ett visst ärende – bland annat i syfte att kunna söka i in- och utresesystemet (se 8 d §) – är emellertid inte begränsade till tredjelandsmedborgare utan omfattar samtliga *utlänningar*, där även EES-medborgare ingår. Om identiteten är oklar kan det alltså tänkas att en sökning utifrån biometriska uppgifter görs även för en EES-medborgare eller annan kategori personer som inte omfattas av den förordning som en sökning genomförs med stöd av. Endast ett påstående om att någon inte är tredjelandsmedborgare kan enligt vår mening inte antas medföra att en sökning inte får utföras, trots att en sökning kan förutsätta att biometriska underlag tas upp. En annan sak är att eventuella sökningar på personer som de facto inte är tredjelandsmedborgare inte kommer att generera några träffar, om systemet som sökningen görs mot endast innehåller uppgifter om sådana medborgare.

Åtgärder som tar sikte på befintliga regelverk bör inte övervägas i detta betänkande

Enligt våra direktiv ska vi i vårt arbete utgå från de förslag som lämnats i annan ordning och som ger Polismyndigheten, Migrationsverket och Skatteverket utökade möjligheter att i olika sammanhang använda biometriska uppgifter. Som vi redogjort för ovan och i kapitel 7 har flera lagstiftningsåtgärder i sådant syfte vidtagits under senare år, vilka

[15] Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004.

tar sikte på ärenden som dessa myndigheter handlägger där en identitet kan behöva etableras. Även med hänsyn tagen till de begränsningar i fråga om personkrets som nämnts ovan är vår sammantagna bedömning att det finns ett brett stöd för myndigheterna att använda biometriska uppgifter för att verifiera identiteten och identifiera tredjelandsmedborgare i sådana ärenden. Redan dessa förhållanden talar enligt vår mening mot att inom ramen för detta betänkande överväga och eventuellt föreslå ytterligare sådant stöd. Behovet av en helhetssyn – vilket har efterfrågats i olika sammanhang – talar enligt vår mening i samma riktning.

Vi kan vidare konstatera att det är fråga om ett relativt svåröverskådligt regelverk där många åtgärder på olika nivåer ska tillämpas av myndigheter med olika uppdrag och förutsättningar. Att föreslå punktinsatser i flera olika författningar, särskilt sådana som rör förslag på bestämmelser som alltjämt är under beredning eller inom kort ska träda i kraft, skulle i sämsta fall kunna bidra till ytterligare svåröverskådlighet. Även detta talar mot att, inom ramen för utredningen, lämna några sådana förslag. Vårt uppdrag är inte heller primärt att lämna förslag som tar sikte på ärenden där identitet etableras i ett inledande skede, utan på åtgärder som stärker kopplingen mellan en sådan grundidentitet och verifiering av identitet, med grund i biometriska uppgifter.

Mot den här bakgrunden anser vi att det, inom ramen för denna utredning, inte bör övervägas att föreslå åtgärder som tar sikte särskilt på de regelverk som i nuläget styr möjligheterna att använda biometriska uppgifter i ärenden där en identitet behöver etableras.

10.3.2 Utökat stöd för att lagra biometriska uppgifter

Vår bedömning

En utökad möjlighet att, i de ärendeslag som vi har beskrivit i kapitel 6, lagra biometriska uppgifter i de register som förs av Polismyndigheten, Migrationsverket och Skatteverket skulle kunna bidra till att motverka att felaktiga, falska och multipla identiteter etableras. Sådana möjligheter har emellertid nyligen varit föremål för översyn och det bör därför inte övervägas att, inom ramen för denna utredning, lämna sådana förslag.

Nyttan av att kunna verifiera identitet eller identifiera en person genom att söka med biometriska uppgifter i en viss databas är i praktiken avhängig av omfattningen, men även typen, av tillgängligt jämförelsematerial. Polismyndigheten, Migrationsverket och Skatteverket har möjlighet att lagra biometriska underlag och biometriska uppgifter i varierande utsträckning, och förslag har lämnats som utökar befintliga möjligheter, bland annat till att omfatta fler ärenden om uppehållstillstånd, vissa ärenden i folkbokföringsverksamheten och ärenden om förvärv av svenskt medborgarskap. Vi har redogjort för detta i avsnitt 8.4 och det sammanfattas i tabellen nedan; med X avses att biometriska underlag eller biometriska uppgifter faktiskt lagras i dagsläget och med 0 avses att författningsförslag har lämnats, men att registret i nuläget inte innehåller sådana underlag eller uppgifter.

Tabell 10.1 Lagring av biometriska underlag och biometriska uppgifter

Register	Biometriska underlag		Biometriska uppgifter	
	Foto	Fingeravtryck	Foto	Fingeravtryck
Migrationsverkets register över fotografier och fingeravtryck		X		X
Den centrala utlänningsdatabasen	X			
Passregistret och registret över nationella id-kort	X		0	
Pass- och identitetskortsregistret[1]	0		0	
Folkbokföringsverksamheten	0	0	0	0

[1] Se promemorian *Ett statligt identitetskort*, Ju2026/01595.

Utifrån det ovanstående bedömer vi att omfattningen av de biometriska underlag och biometriska uppgifter som kan lagras i befintliga register i nuläget får anses i viss mån begränsad. En utökad möjlighet att lagra biometriska underlag och biometriska uppgifter som tagits fram i fler ärendeslag skulle potentiellt kunna bidra till att motverka att felaktiga, falska och multipla identiteter etableras. De nuvarande möjligheterna har emellertid varit föremål för överväganden i flera lagstiftningsärenden under senare år,[16] och vårt uppdrag omfattar inte att göra en översyn av detta. Det är också i nuläget svårt att

[16] Se bland annat prop. 2025/26:261, prop. 2025/26:263 och *Anpassning av svensk rätt till den reviderade VIS-förordningen*, prop. 2024/25:176.

utvärdera vilken effekt lämnade förslag kan antas få; om biometriska underlag och biometriska uppgifter lagras i ett visst register är också avhängigt av att myndigheten har tekniska förutsättningar att utnyttja de rättsliga möjligheter som finns. Vad vi anfört ovan angående lämpligheten i att, inom ramen för denna utredning, föreslå punktinsatser i flera olika författningar, särskilt sådana som rör förslag på bestämmelser som alltjämt är under beredning, har enligt vår bedömning bäring även på överväganden som tar sikte på lagring av biometriska underlag och biometriska uppgifter. I de ärenden där en identitet behöver etableras görs jämförelser med biometriska underlag och biometriska uppgifter för att verifiera identitet eller identifiera någon dessutom i stor utsträckning mot EU-gemensamma system. Behovet av att utöka möjligheterna att lagra biometriska underlag och/eller uppgifter i de register som förs av Polismyndigheten, Migrationsverket och Skatteverket – i syfte att främja en korrekt etablering av en grundidentitet – kan därför inte anses lika framträdande. Vidare anser vi – vilket vi återkommer till i avsnitt 10.6 – att dessa register inte bör ligga till grund för en utökad möjlighet för andra aktörer än Polismyndigheten, Migrationsverket och Skatteverket att använda biometriska uppgifter för att verifiera identitet. Det saknas därför anledning att på den grunden överväga att lämna förslag som medför utökade lagringsmöjlighet i dessa register, i sådana ärenden som vi redogjort för i kapitel 6.

Sammantaget anser vi att det inte bör övervägas att, inom ramen för denna utredning, lämna förslag som tar sikte på en utökad möjlighet att lagra biometriska uppgifter i de register som förs av Polismyndigheten, Migrationsverket och Skatteverket.

10.4 Utökad användning av biometri är nödvändig

Vår bedömning

Åtgärder som innebär utökad användning av biometriska uppgifter, av fler aktörer och i fler ärendeslag och situationer än i dag, bör vara utgångspunkten för våra fortsatta överväganden.

Som nämnts i inledningen till det här kapitlet är vårt uppdrag att lämna förslag som stärker kopplingen mellan en fastställd grundidentitet och verifiering av identitet med grund i biometriska uppgifter. Att kunna använda biometriska underlag och biometriska uppgifter som finns lagrade i ett register eller i en handling utgör en viktig komponent i att främja att korrekta identitetsuppgifter registreras i ett ärende där en grundidentitet behöver etableras, men även för att motverka identitetsmissbruk – särskilt utnyttjande av identiteter – i andra sammanhang. Möjligheter för myndigheter som exempelvis Försäkringskassan, Pensionsmyndigheten och Centrala studiestödsnämnden att använda biometriska uppgifter för att jämföra dem mot sådana uppgifter som är lagrade i ett register eller i en handling skulle kunna motverka att identiteter utnyttjas på ett sätt som inte är möjligt genom endast alfanumeriska sökningar. Detta med hänsyn till att en alfanumerisk sökning som utgångspunkt endast kan ge en upplysning om att det finns *någon* person registrerad med den uppgivna identiteten, det vill säga en viss kombination av namn, födelsetid och medborgarskap. Enligt vår mening är risken stor att en sådan sökning också genererar flera träffar och ytterligare information behövs då för att på ett tillförlitligt sätt koppla ihop träffen med den individ som myndigheten möter. Detta gäller även om en sökning görs med en unik alfanumerisk nyckel av något slag som säkerställer att endast en träff returneras (se även avsnitt 11.3). En alfanumerisk sökning mot ett register bör därför – vilket vi redogjort för i avsnitt 7.2.1 – i första hand ses som ett sätt att lokalisera en träff, mot vilken en biometrisk verifiering kan göras.

Med detta sagt kan även en jämförelse av alfanumeriska uppgifter ha en självständig funktion för att motverka i vart fall utnyttjande av identiteter. Om en sökning görs med en unik alfanumerisk nyckel av något slag, som garanterar att endast en träff returneras, och det är uppenbart att en lagrad ansiktsbild som är kopplad till träffen inte stämmer överens med den person som myndigheten möter, kan ett försök att använda en falsk identitet eller någon annans identitet upptäckas, på samma sätt som om den enskilde hade försökt legitimera sig med en fotoförsedd identitetshandling som avser någon annan. Verifiering av identitet kan också främjas genom att en jämförelse görs mellan andra sidouppgifter som är kopplade till träffen och de som den person som myndigheten möter har lämnat.

För att tillförlitligt kunna koppla ihop en individ med information om identitet som är lagrad i ett register eller i en handling behöver däremot biometriska uppgifter kunna användas. Vi anser med hänsyn till detta att sådana åtgärder som innebär en utökad användning av biometriska uppgifter bör vara utgångspunkten för våra vidare överväganden. Biometriska uppgifter har lyfts fram som ett av de mest effektiva verktygen för att bekämpa identitetsrelaterad brottslighet.[17] De är unika för varje individ och möjliggör, till skillnad från identitetshandlingar som kan stjälas, manipuleras eller förfalskas, en direkt koppling till en individ. När identiteter kan verifieras biometriskt blir det svårare att dölja sig bakom en falsk identitet och det ökar möjligheten att följa en individ och till ansvarstagande.

Biometrisk verifiering kan kopplas till en enhetlig digital identitet som följer individen över tid, vilket försvårar möjligheten att byta identitet för att exempelvis undgå ansvar, skulder eller straff, och innebär att det går att upptäcka om en individ uppträder under olika identiteter i olika sammanhang. Det är enligt vår mening viktigt att dessa möjligheter inte är förbehållna Polismyndigheten, Migrationsverket och Skatteverket eller begränsade till de ärenden där en identitet kan behöva etableras av dessa myndigheter. Biometrisk identifiering – det vill säga att biometriska uppgifter används för att göra en en-till-många-jämförelse mot uppgifter i ett register – skulle även kunna främja att multipla identiteter upptäcks vid handläggningen av andra ärendeslag än sådana där en identitet kan behöva etableras.

10.5 Verifiering mot handlingar

Verifiering av identitet sker i många fall med hjälp av identitetshandlingar, eller andra handlingar som innehåller identitetsuppgifter. Ett sätt är att okulärt jämföra det fotografi som finns på handlingen med den person som en myndighet eller någon annan aktör möter för att koppla individen till de uppgifter om identitet som finns på handlingen. Detta är inte en helt tillförlitlig metod och möjliggör att identiteter utnyttjas, till exempel genom så kallade look-a-likes. Om handlingen innehåller biometriska underlag kan däremot en kontroll mot de biometriska uppgifter som kan tas fram ur dessa på ett mer till-

[17] Brottsförebyggande rådet, Rapport 2016:9, *Bedrägeribrottsligheten i Sverige*, s. 148 och 163.

förlitligt sätt säkerställa kopplingen mellan identitetshandlingen och innehavaren.

10.5.1 Tillgång till identitetshandlingar

Vår bedömning

En utökad möjlighet för myndigheter att kräva att en person överlämnar en identitetshandling som han eller hon innehar kan stärka kopplingen mellan en etablerad identitet och verifiering av identitet.

Tvångsåtgärder för att få tillgång till identitetshandlingar utgör ingripande åtgärder, som får vidtas endast i särskilt angivna situationer. Det bör därför inte övervägas att, inom ramen för denna utredning, lämna förslag som utökar befintliga möjligheter att vidta sådana åtgärder.

En del i att kunna upptäcka identitetsmissbruk är att myndigheter kan kräva att få tillgång till identitetshandlingar som den person vars identitet ska kontrolleras innehar. Ett sådant behov gör sig ofta gällande i ärenden där en identitet behöver etableras, särskilt i ärendeslag där ett krav på styrkt identitet inte är en förutsättning för att ansökan ska beviljas; den enskilde har då inte ett naturligt incitament att självmant överlämna identitetshandlingar av den anledningen. Som exempel på ett sådant ärende kan nämnas en ansökan om uppehållstillstånd på grund av behov av internationellt skydd. Vid verifiering av identitet i andra situationer är tillgången till identitetshandlingar naturligtvis också av stor betydelse. I många sammanhang kan det med fog antas att verifieringen görs endast mot identitetshandlingen och en ansiktsbild som finns på den. Identitetshandlingar kan emellertid också innehålla biometriska underlag, lagrade på ett chip i handlingen. Det kan även vara möjligt att extrahera biometriska uppgifter från en ansiktsbild som är synlig på handlingen, vilka kan användas för att biometriskt verifiera identiteten genom en jämförelse med andra sådana uppgifter. I propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* lämnades förslag om att Skatteverket ska få just en sådan möjlighet, att använda en på handlingen synlig ansiktsbild, vid en identitetskontroll i ett ärende i folkbokföringsverksamheten.[18]

[18] Prop. 2025/26:261, s. 103.

Stödet för myndigheter att få tillgång till identitetshandlingar genom en uttrycklig skyldighet i författning för den enskilde att överlämna sådana handlingar, indirekt genom krav på att identiteten ska styrkas genom uppvisande av en godtagbar identitetshandling eller genom särskilda åtgärder, är emellertid begränsat till ett fåtal ärendeslag och situationer. Dessa omfattar i första hand ärendeslag där en identitet kan behöva etableras, vilka vi har redogjort för i kapitel 6, men även ärenden om ansökan om pass eller nationellt identitetskort[19], och det statliga identitetskort som föreslagits i promemorian *Ett statligt identitetskort*.[20] I andra ärendeslag saknas däremot ofta stöd för en myndighet att *kräva* att den enskilde överlämnar en identitetshandling; exempelvis finns det inga bestämmelser som uttryckligen ger Försäkringskassan och Pensionsmyndigheten rätt att ställa ett sådant krav i ett ärende om en socialförsäkringsförmån. Vi anser att behovet av att kunna få tillgång till en identitetshandling – i vart fall i en situation då identiteten av olika skäl behöver verifieras – kan vara framträdande även i sådana ärenden. Enligt vår bedömning skulle en utökad möjlighet för myndigheter att få tillgång till en identitetshandling som den individ som myndigheten möter innehar därmed kunna stärka kopplingen mellan etablerad identitet och verifiering av identitet.

Överväganden om ett utökat stöd för att få tillgång till identitetshandlingar bör enligt vår uppfattning dock begränsas till att avse en utökad rätt för myndigheter att kräva att en identitetshandling som den enskilde innehar överlämnas eller görs tillgänglig på något annat sätt. Tvångsåtgärder av sådant slag som i vissa situationer får vidtas med stöd av 9 kap. utlänningslagen – kroppsvisitation och undersökning av en utlännings bagage – utgör däremot ett mer betydande ingrepp i rätten till skydd för privatlivet och måste både motiveras av ett angeläget samhälleligt behov och stå i rimlig relation till det intresse åtgärden är avsedd att tillgodose.[21] Genomförandet av sådana åtgärder är vidare normalt förbehållet polisman. Dessa omständigheter innebär, som vi ser det, att det varken är möjligt eller lämpligt att – inom ramen för vårt uppdrag – överväga att lämna förslag om att sådana tvångsåtgärder generellt sett ska kunna vidtas av en bred skara myndigheter, i ärenden av vitt skilda slag.

[19] Se 3 kap. 2 § Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort, PMFS 2021:3.
[20] Ju2026/01595.
[21] *Effektivare verktyg vid inre utlänningskontroll,* prop. 2023/24:12, s. 15.

10.5.2 Utökad användning av biometriska uppgifter

Vår bedömning

En utökad möjlighet för myndigheter att kontrollera biometriska uppgifter mot handlingar kan stärka kopplingen mellan etablerad identitet och verifiering av identitet.

I avsnitt 7.4.2 har vi redogjort för de möjligheter som Polismyndigheten, Migrationsverket och Skatteverket har att, i vissa ärendeslag, kontrollera biometriska uppgifter mot identitetshandlingar och vissa andra handlingar som innehåller identitetsuppgifter. Exempelvis kan handlingar som har utfärdats av Migrationsverket, bland annat uppehållstillståndskort, kontrolleras av en polisman enligt 9 kap. 8 b § utlänningslagen vid gränskontroller och i samband med en inre utlänningskontroll, och Migrationsverket har föreslagits få rätt att ta upp biometriska underlag i vissa ärenden om medborgarskap för att jämföra dessa mot de uppgifter som finns lagrade i sökandens uppehållstillståndskort.[22] En motsvarande möjlighet har föreslagits för ärenden om registrering av EES-medborgare.[23] Om en handling innehåller en ansiktsbild eller ett lagringsmedium med biometriska underlag ur vilka biometriska uppgifter kan tas fram, kan en jämförelse av dem med biometriska uppgifter som har tagits fram ur biometriska underlag som tagits upp av en person på plats säkerställa en koppling mellan handlingen och innehavaren. Användning av biometriska uppgifter på detta sätt kan motverka att identiteter utnyttjas genom missbruk av identitetshandlingar, och ger enskilda bättre möjligheter att skydda sin identitet. Eftersom verifieringen görs mot uppgifter som finns lagrade i handlingen, som den enskilde förfogar över, utgör kontrollen också ett mindre integritetsintrång än om jämförelsen görs mot tidigare lagrade biometriska underlag eller biometriska uppgifter i en databas. Kontroller av biometriska uppgifter som kan tas fram ur biometriska underlag som är lagrade i handlingar kan därmed anses utgöra en mycket betydelsefull komponent i att motverka identitetsmissbruk.

Vi kan konstatera att metoden i praktiken endast får användas av ett fåtal myndigheter, i ett begränsat antal ärendeslag och situationer.

[22] Prop. 2025/26:263, s. 129 ff.
[23] SOU 2026:9, s. 194.

Detta trots att det kan antas vara relativt vanligt att enskilda legitimerar sig med identitetshandlingar som innehåller biometriska underlag även i ärenden och situationer där detta inte utgör ett krav, exempelvis vid kontakt med myndigheter som handlägger ärenden om förmåner av olika slag. Som vi lyft fram i avsnitt 9.2.4 gör Försäkringskassan och Pensionsmyndigheten i nuläget begränsade, eller inga, kontroller för att säkerställa att en person som ansöker om en förmån hör ihop med det personnummer som används; vid kontrollen av identitet förlitar sig dessa myndigheter normalt på den e-legitimation den enskilde använt och de säkerhetskrav som utfärdaren av e-legitimationen föreskriver. Även om sådana kontakter alltså i allt större utsträckning i dag sker på digital väg anser vi emellertid att utökade *möjligheter* för myndigheter att biometriskt verifiera identitet mot handlingar – när detta är motiverat – kan vara ett effektivt sätt att stärka kopplingen mellan etablerad identitet och verifiering av identitet. Denna metod för att verifiera identitet är emellertid inte utan begränsningar.

En svaghet med en biometrisk jämförelse mot en viss handling är att metoden inte gör det möjligt att upptäcka om en person använder sig av multipla identiteter.[24] Det kräver att *identifiering* med hjälp av biometriska uppgifter kan genomföras mot ett större urval uppgifter, det vill säga uppgifter som är lagrade i ett register av något slag. 2017-års ID-kortsutredning anförde att för att kunna stävja den brottslighet som beror på att identitetshandlingar utfärdas för en och samma person i flera identiteter finns ingen annan effektiv metod än sökning på ansiktsbilderna. Det ansågs därför finnas tungt vägande skäl som talar för att möjliggöra sådana sökningar i det id-kortsregister som föreslogs av utredningen.[25] Sådana sökningar ska också vara möjliga att göra i det pass- och identitetskortsregister som föreslagits i promemorian *Ett statligt identitetskort.*[26] En möjlighet att jämföra biometriska uppgifter på det sättet i samband med utfärdandet av en identitetshandling kan effektivt motverka att handlingar utfärdas i olika identiteter till en och samma person. Som vi anfört i avsnitt 10.3.1 bedömer vi också att det finns ett brett rättsligt stöd för att använda biometriska uppgifter i syfte att motverka multipla identiteter i de ärenden där en grundidentitet kan behöva etableras. Att biometrisk verifiering av identitet mot handlingar inte på samma sätt kan motverka sådana

[24] *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 49 och *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 68.
[25] SOU 2019:14, s. 297.
[26] Ju2026/01595, s. 14 f.

former av identitetsmissbruk framstår därför, enligt vår mening, inte som någon mer framträdande nackdel, utan de olika åtgärderna kan komma att komplettera varandra, i olika delar av en sammanhållen identitetsförvaltning.

Vidare förutsätter en verifiering av identitet med biometriska uppgifter mot en identitetshandling att den enskilde aktivt medverkar i flera led. För det första ska personen tidigare ha ansökt om och fått en identitetshandling som innehåller biometriska underlag utfärdad. En viss mindre andel av de personer som vi – enligt vår bedömning i kapitel 12 – anser har sådan anknytning till Sverige att deras identitet kan behöva verifieras, kommer att sakna sådana handlingar eller en möjlighet att få dem utfärdade. Bland dessa kan vissa utlänningar som har tilldelats ett samordningsnummer nämnas. Det kan dock antas att en stor andel av den personkrets vars identitet myndigheter kan behöva verifiera biometriskt har en identitetshandling. Verifiering av identitet mot ett register i form av ett identitetsindex (se avsnitt 10.7) kommer, enligt våra överväganden i avsnitt 13.3, för svenska medborgare som bor i Sverige också att förutsätta att den enskilde har ansökt om och fått en identitetshandling utfärdad. Vidare ska personer som beviljas uppehållstillstånd i Sverige som är giltigt i mer än sju dagar få ett uppehållstillståndskort utfärdat, vilket enligt våra överväganden också bör kunna användas för att verifiera identitet biometriskt (se avsnitt 13.3.5). Att den enskilde ska ha ansökt om och fått en identitetshandling – eller annan handling som innehåller biometriska underlag – utfärdad framstår mot den här bakgrunden inte som en reell begränsning med metoden i praktiken.

För det andra förutsätts att personen har ett incitament att uppge för myndigheten att han eller hon har en handling som innehåller biometriska underlag samt att överlämna handlingen, eller på annat sätt göra den tillgänglig, för kontroll. Bristande medverkan vid verifiering av identitet medför i nuläget en konkret, i författning eller föreskrifter reglerad, konsekvens endast i vissa särskilda ärendeslag, exempelvis genom att en ansökan om uppehållstillstånd eller pass kan avslås redan på grunden att personen inte har styrkt sin identitet eller medverkat till detta på angivet sätt (se MIG 2011:11 och 7 § 1 passlagen). Mer vanligt är emellertid att detta inte är reglerat. I sådana fall skulle det kunna tänkas att en myndighet faller tillbaka på den möjlighet som följer av 20 § förvaltningslagen (2017:900) att – efter föreläggande om att avhjälpa brister – avvisa framställningen.

Dessa omständigheter medför enligt vår bedömning att det finns en viss risk för att effekten av en möjlighet att biometriskt verifiera identitet mot handlingar i praktiken blir begränsad, något som lyftes fram av remissinstanserna i förarbetena till 26 b § folkbokföringslagen.[27] Till detta kommer att den enskilde behöver medverka till att lämna biometriska underlag som kan användas vid jämförelsen med de uppgifter som kan tas fram ur de biometriska underlag som finns lagrade i eller synliga på handlingen. Det förutsätts också att utrustning för att skanna identitetshandlingen, och för att ta upp biometriska underlag, finns och fungerar. Detta gäller emellertid också vid en kontroll mot ett identitetsindex eller ett annat register. En identitetshandling som lämnas över för kontroll kan emellertid vara skadad, vilket gör att det inte går att läsa av de biometriska underlag som är lagrade i den. När det gäller sistnämnda omständighet kan vi notera att av uppgifter från Skatteverket framgår att vid kontroller i ärenden om flyttning till Sverige och om samordningsnummer under perioden juni 2024 till och med mars 2025 överlämnades omkring 179 000 pass, identitetskort och uppehållstillståndskort med lagringsmedium, men att de biometriska underlagen inte kunde läsas i drygt 17 000 av dessa handlingar. Förslag om att Skatteverket ska kunna ta fram biometriska uppgifter från en synlig ansiktsbild på en handling har därför lämnats (se avsnitt 10.5.1). Sådana åtgärder kan bidra till att motverka problem av nyss nämnda slag.

En utökad möjlighet att verifiera identitet med hjälp av biometriska uppgifter i en identitetshandling blir alltså i viss mån avhängig av den enskildes aktiva medverkan och huruvida en handling är i maskinläsbart skick, så att biometriska underlag i handlingen kan göras tillgängliga. Denna metod för att verifiera identitet är dessutom en åtgärd som i första hand tar sikte på att kontrollera om handlingen är utfärdad till innehavaren, och är som vi ser det inte optimal för att i ett bredare perspektiv motverka användningen av multipla identiteter. Verifiering av identitet kan också behöva ske utan tillgång till en identitetshandling. Metoden har dock fördelen att den kan användas även i fall då det inte finns tidigare lagrade uppgifter i ett register att genomföra en biometrisk verifiering mot.

De begränsningar avseende biometrisk verifiering mot handlingar som vi redogjort för ovan är, enligt vår mening, inte av sådan karaktär och omfattning att sådan verifiering inte framstår som ett relevant

[27] Prop. 2021/22:217, s. 44 och 47.

eller ineffektivt alternativ för att stärka kopplingen mellan etablerad identitet och verifiering av identitet. Vissa av de svårigheter som pekats på ovan kan som vi ser det också motverkas genom att lämpliga tekniska system används, att även en synlig ansiktsbild kan användas för den biometriska jämförelsen och att det finns en möjlighet att – exempelvis genom föreläggande som är kopplat till en reell konsekvens – förmå den enskilde att medverka. Vi anser därför att det finns anledning att utreda en möjlighet – för fler aktörer och i andra situationer än vad som gäller i dag – att kontrollera biometriska uppgifter mot identitetshandlingar, och vissa andra handlingar som innehåller ett lagringsmedium med biometriska underlag (se avsnitt 19.2.1). En sådan möjlighet att verifiera identitet med hjälp av biometriska jämförelseunderlag som den enskilde förfogar över medför, enligt vår bedömning, ett betydligt mindre integritetsintrång än ett system med ett identitetsindex, som förutsätter lagring av biometriska uppgifter i ett centralt register. Det framstår därför som relevant och lämpligt att utvärdera en mer generell möjlighet att verifiera identitet biometriskt mot handlingar, för att se i vilken utsträckning en sådan möjlighet kan bidra till att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet.

10.6 Verifiering mot befintliga register

Polismyndigheten, Migrationsverket och Skatteverket för i dag register som innehåller, eller föreslås få innehålla, biometriska underlag och biometriska uppgifter. Ett alternativ som kan övervägas för säkrare verifiering av identitet är en lösning som bygger på befintliga register, för att snabbare kunna ta ett system för verifiering av identitet som använder biometriska uppgifter i bruk. Vi anser emellertid att en sådan lösning inte är lämplig, på de skäl vi redogör för nedan. Vi anser att det inte heller är möjligt att använda EU-gemensamma informationssystem direkt för att möjliggöra verifiering av identitet i ett bredare sammanhang (se avsnitt 10.6.3).

10.6.1 Stöd för fler aktörer att använda lagrade biometriska uppgifter

Vår bedömning

Det är inte lämpligt att införa en möjlighet för andra aktörer än Polismyndigheten, Migrationsverket och Skatteverket att använda biometriska uppgifter för att jämföra dessa med sådana uppgifter i befintliga register hos dessa myndigheter.

De befintliga register som skulle kunna komma i fråga för att verifiera identitet med biometriska uppgifter är i första hand Migrationsverkets register över fingeravtryck och fotografier, den centrala utlänningsdatabasen – som innehåller ansiktsbilder – samt passregistret och registret över nationella identitetskort. Dessa innehåller uppgifter om en stor mängd personer; i passregistret finns ansiktsbilder för drygt sex miljoner svenska medborgare som har fått pass utfärdat och i de förstnämnda registren finns biometriska underlag i form av ansiktsbilder samt biometriska uppgifter i form av fingeravtryck lagrade om ett stort antal utländska medborgare. I folkbokföringsverksamheten finns det i nuläget inte några biometriska underlag eller biometriska uppgifter. Detta innebär dock inte att folkbokföringen inte skulle kunna utgöra ett potentiellt jämförelseunderlag, särskilt med hänsyn till att förslag har lämnats i propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* om att myndigheten ska få lagra biometriska underlag och biometrisk uppgifter som tagits upp och fram i samband med en identitetskontroll i vissa ärenden om folkbokföring och samordningsnummer.[28] Flera faktorer talar emellertid, enligt vår uppfattning, mot att det är lämpligt att införa ett system som innebär en utökad rätt att söka med biometriska uppgifter i befintliga register som förs av Polismyndigheten, Migrationsverket och Skatteverket.

[28] Prop. 2025/26:261, s. 44.

Befintliga register får användas för begränsade ändamål

Ovan nämnda register förs och får användas endast för vissa uppräknade ändamål. Bestämmelser som reglerar detta finns till exempel i 15 § utlänningsdatalagen, 23 § passförordningen (1979:664), 14–18 §§ förordningen (2005:661) om nationellt identitetskort och 5–7 §§ folkbokföringsdatalagen (2026:126). För att befintliga register, och uppgiftssamlingar, ska kunna få användas av en bredare krets av aktörer för att verifiera identitet i olika ärendeslag krävs att ändamålsbestämmelserna i respektive register ses över och eventuellt kompletteras. I annat fall riskerar behandlingen att strida mot grundläggande principer i dataskyddsförordningen[29], nämligen principen om ändamålsbegränsning i artikel 5.1 b. För att ett intrång i den personliga integriteten – som det innebär om en större krets myndigheter får tillgång till biometriska underlag och biometriska uppgifter som lagrats i flera olika register – överhuvudtaget ska vara proportionerligt krävs, enligt vår mening, att intrånget är förutsebart, och förutsätter att en reglering som möjliggör ett sådant informationsutbyte tydligt anger i vilka situationer det får ske. Sådana bedömningar kompliceras också av att förslag om ett nytt statligt identitetskort, som ska ersätta det nationella identitetskortet, har lämnats; det skulle då vara fråga om att utvärdera och föreslå ändringar avseende ett register som i dag inte existerar. Ju fler register – som i nuläget förs för vitt skilda ändamål – som ska ”öppnas upp”, desto svårare kan krav på proportionalitet och förutsebarhet antas bli att uppnå. Att ge ett större antal myndigheter tillgång till flera befintliga – och potentiellt framtida – register som förs för olika syften och med olika innehåll skulle alltså sannolikt kräva omfattande och komplexa författningsåtgärder, vilka riskerar att bidra ytterligare till ett redan svåröverskådligt regelverk. Detta kan i sig påverka möjligheten och viljan att använda de rättsliga verktyg som eventuellt införs, vilket riskerar att leda till att effekten av de tänkta åtgärderna i praktiken går om intet.

Fler personuppgifter än nödvändigt kan komma att behandlas

I artikel 5.1 c i dataskyddsförordningen anges att vid behandling av personuppgifter ska uppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Fler

[29] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

uppgifter än nödvändig ska alltså som utgångspunkt inte behandlas. Sett i ljuset av de åtgärder som vi nu överväger innebär detta att sökningar med biometriska uppgifter för att verifiera identitet som utgångpunkt bör göras mot register som endast innehåller de uppgifter som behövs för ett sådant ändamål, eller för att identifiera någon när en verifiering inte är möjlig.

De register som nämnts ovan innehåller för det första en mängd uppgifter som är av sådan art att de inte kan antas krävas för detta ändamål. Exempelvis registreras information om folkbokföringsadress, födelseort och civilstånd i folkbokföringsverksamheten. Som vi återkommer till i kapitel 11 anser vi att ett system för att verifiera identitet med hjälp av biometriska uppgifter bör innehålla en mycket begränsad uppsättning uppgifter.

Befintliga register innehåller dessutom information om individer som det helt kan saknas behov av att verifiera identiteten för, det vill säga personer som varken har hemvist eller är bosatta i Sverige eller på annat sätt har en anknytning till landet. Exempelvis kan det vara fråga om en person vars fingeravtryck har tagits upp och lagrats med stöd av 9 kap. 8 § 3 utlänningslagen och 15 § utlänningsdatalagen, på grund av att personen har tagits i förvar för att ett beslut om avvisning ska kunna verkställas; det kan då helt saknas anledning att anta att personen kommer att vistas i Sverige på sätt som medför att hans eller hennes identitet kan komma att behöva verifieras genom en sökning mot Migrationsverkets register (angående personkrets, se kapitel 12). Den centrala utlänningsdatabasen innehåller uppgifter inte bara om utlänningar som har sökt eller söker svenskt medborgarskap eller som har beviljats tillstånd för att besöka, bo, arbeta eller studera i Sverige, utan även de som har fått avslag på sina ansökningar om till exempel uppehålls- eller arbetstillstånd. Även utlänningar som avvisats vid gränsen, tagits i förvar eller dömts till utvisning från Sverige är registrerade. Det handlar sammantaget om en omfattande mängd uppgifter om ett stort antal personer.[30] När det gäller folkbokföringsverksamheten kan vi konstatera att den innehåller uppgifter även om avlidna personer, vars identitet mycket sällan kan antas behöva verifieras.

Vid en sökning med alfanumeriska uppgifter mot befintliga register i syfte att kunna lokalisera en träff mot vilken en biometrisk verifiering kan genomföras, och i synnerhet vid en en-till-många-jämförelse för att identifiera en individ, skulle det därmed finnas en tydlig risk

[30] *Utlänningsdatalag*, prop. 2015/16:65, s. 29 f. och 37.

för att en stor mängd personuppgifter behandlas i onödan. Även om det kan tänkas vara möjligt att tekniskt utforma ett sökverktyg så att endast begränsade delar av uppgifterna i registren behandlas vid en sökning, skulle detta leda till komplexitet i utformningen och tillämpningen. Det säkerställer, som vi ser det, inte heller att personuppgifter inte behandlas i onödan, på samma sätt som om uppgifterna inte finns lagrade från början i det register som en sökning kan komma att ske mot. Sammantaget anser vi att principen om uppgiftsminimering talar starkt mot att bygga ett system för verifiering av identitet med biometriska uppgifter på en utökad tillgång till befintliga register.

Bristande tillförlitlighet och problem av praktisk och teknisk art

Att utgå från befintliga register är enligt vår mening också vanskligt med hänsyn till tillförlitlighet och praktisk tillämpning. Det är känt att befintliga register innehåller såväl felaktiga som multipla identiteter. Som nämnts i avsnitt 9.2.5 finns uppgifter om att Migrationsverket år 2017 gjorde bedömningen att det då fanns nära 60 000 individer registrerade med två eller flera kända identiteter hos myndigheten och att mörkertalet var stort. I betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* lyftes fram att såväl Skatteverket som Migrationsverket har uppgett att det är mycket svårt att uppskatta omfattningen av falska, felaktiga och multipla identiteter i respektive myndighets verksamhet.[31] Tillförlitligheten i de sökresultat som en verifiering mot befintliga register skulle generera kan med hänsyn till detta antas påverkas negativt, särskilt som tanken är att detta ska kunna användas av en bred krets av aktörer; dessa ska inte behöva vidta åtgärder för att utreda om en viss träff är tillförlitlig eller inte.

För att en verifiering med biometriska uppgifter mot befintliga register ska kunna returnera ett tillförlitligt resultat behöver dessutom en unik individ kunna lokaliseras, mot vilken biometriska uppgifter kan jämföras. Detta skulle, som vi ser det, i första hand kunna uppnås genom att varje individ får en unik alfanumerisk nyckel (se avsnitt 11.3), innebärande att en individ endast kan ha *en* sådan nyckel och att den är bestående, även om personen till exempel tilldelas ett personnummer efter att tidigare ha haft ett samordningsnummer. I annat fall skulle verifiering i många fall förutsätta att lokaliseringen

[31] SOU 2025:75, s. 481.

görs genom en sökning med biometriska uppgifter i samtliga register, det vill säga genom *identifiering*, för att hitta den individ vars identitet ska verifieras. Detta är enligt vår mening inte lämpligt (se avsnitt 7.4.1), inte minst med hänsyn till vad vi anfört ovan om den ”överskottsinformation” som kan anses finnas i befintliga register. Befintliga register innehåller inte en unik alfanumerisk nyckel, utan i stället identitetsbeteckningar eller Migrationsverkets individnummer. Förekomsten av multipla identiteter i befintliga register innebär att vissa personer har mer än ett personnummer eller samordningsnummer alternativt flera individnummer; en träff i ett register efter en sökning med till exempel ett personnummer ger därmed inte nödvändigtvis träff på en unik individ. För de individer som redan finns i befintliga register är det enligt vår bedömning inte möjligt att skapa unika alfanumeriska nycklar, ens efter en manuell genomgång och jämförelse av samtliga uppgifter för att sammankoppla multipla identiteter som avser samma individ. Det kan också tänkas att en sådan nyckel skapas i befintliga register i samma situationer som vi bedömer att en nyckel bör skapas i kapitel 13. Dessa nycklar skulle då behöva spridas till samtliga befintliga register där en viss individ förekommer och kopplas samman med individen. En sådan ordning framstår enligt vår mening som komplex. Någon tidsvinst i att använda befintliga register för biometrisk verifiering – jämfört med att ett identitetsindex byggs upp – har vi också svårt att se.

Även med utgångspunkten att lokalisering av en viss individ skulle kunna göras i befintliga register med hjälp av en unik identitetsnyckel eller genom att sökningar görs med person- eller samordningsnummer – eller möjligen det individnummer Migrationsverket använder – kvarstår svårigheter i hur en sökning skulle kunna genomföras. Två huvudsakliga alternativ är aktuella.

Ett alternativ är att myndigheter som behöver verifiera identitet får möjlighet att genomföra sökningar direkt i befintliga register, antingen genom direktåtkomst eller i form av en fråga-svarstjänst. Vi anser att detta inte är en realistisk väg att gå. Direktåtkomst till passregistret eller Migrationsverkets fingeravtrycksregister, på liknande sätt som är möjligt via en prenumerationstjänst på Statens personadressregister (SPAR), är enligt vår bedömning överhuvudtaget inte lämplig, och skulle vara svår att förena med dataskyddsförordningen. Det skulle också ställa krav på den som vill verifiera identitet att sammanställa och värdera information från flera register, vilket

kan påverka tillförlitligheten i verifieringen negativt. Vidare skulle det kräva antingen manuella arbetsinsatser eller att varje aktör tar fram tekniska lösningar för att sammanställa sökresultaten.

Det andra alternativet är att sökning sker mot någon form av gemensam portal, som i sin tur söker i underliggande register och sammanställer ett svar till den aktör som vill verifiera identitet. En sådan lösning innebär att information behöver eftersökas och hämtas från befintliga register varje gång en verifiering görs, vilket belastar dessa. Det framstår därför inte heller som en lämplig lösning. Vidare kan vi konstatera att vissa befintliga register inte innehåller, eller ska innehålla, biometriska uppgifter, utan endast biometriska underlag. Det innebär att de biometriska uppgifterna skulle behöva skapas i samband med varje enskild sökning, för att en biometrisk verifiering ska kunna genomföras. I betänkandet *Biometri – för en effektivare brottsbekämpning* anfördes, i samband med överväganden om sökningar med biometriska uppgifter mot Vägtrafikregistret, att en sådan lösning skulle innebära att registret inte kan användas för andra ändamål under tiden sökningen genomförs och att det skulle kräva att det skapas en kopia av registret som kan användas för sådana sökningar, vilket skulle ta omfattande resurser i anspråk.[32] Vi bedömer att motsvarande skulle göra sig gällande i fråga om de register som nu är aktuella, bland annat den centrala utlänningsdatabasen, i vart fall i samband med en en-till-många-jämförelse. Att i stället på förhand ta fram de biometriska uppgifterna skulle förutsätta att de lagras i ett nytt, eventuellt gemensamt, register. Vi har då svårt att se någon avgörande skillnad jämfört med ett identitetsindex, annat än att det förra alternativet alltjämt bygger på, och kontinuerligt behöver uppdateras mot, flera olika underliggande register. Att en lösning av det slaget skulle vara mindre komplex eller kostnadskrävande än att bygga upp ett fristående, nytt, identitetsindex framstår inte som sannolikt.

Sammantagen bedömning

En uppenbar fördel med att bygga ett system för verifiering av identitet mot befintliga register är att de redan innehåller en mängd uppgifter, som potentiellt skulle kunna användas för detta ändamål. Som vi redogjort för ovan medför detta dock samtidigt betänkligheter i

[32] SOU 2023:32, s. 476 f.

fråga om principer om ändamål och uppgiftsminimering enligt dataskyddsförordningen. Utöver sådana faktorer finns det omständigheter av teknisk och praktisk art som kan medföra att även ett system som bygger på de register som Polismyndigheten, Migrationsverket och Skatteverket för riskerar att ge icke tillförlitliga svar och bli både komplext och kostsamt. Det skulle även vara svårare att peka ut vem som är ansvarig för informationen, eftersom den bygger på uppgifter i register som finns hos tre olika myndigheter. Lösningen främjar inte heller en sammanhållen syn på identitetsförvaltningen och skulle, som vi ser det, inte råda bot på att myndigheterna i dag arbetar alltför stuprörsformat med frågor om identitet, utifrån sina respektive uppdrag. I Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* lyftes det fram att det finns mycket data hos de olika myndigheterna, men inget centralt register eller någon myndighet som håller ihop helheten.[33] Både informationen som sådan och ansvaret är i hög grad fragmenterat. Med ett system för verifiering av identitet med hjälp av biometriska uppgifter som bygger på befintliga register skulle detta problem kvarstå.

Vid en sammantagen bedömning anser vi därför att verifiering av identiteten med hjälp av biometriska uppgifter, mot ett register, inte bör ske mot befintliga register.

10.6.2 Utökat informationsutbyte mellan Polismyndigheten, Migrationsverket och Skatteverket

Vår bedömning

Ett eventuellt behov för Polismyndigheten, Migrationsverket och Skatteverket av utökad tillgång till biometriska uppgifter i de register som dessa myndigheter för bör utredas i annan ordning.

Det har under vårt arbete förts fram önskemål om ökad möjlighet för exempelvis Polismyndigheten att använda biometriska uppgifter för att i ärenden som inte avser etablering av identitet göra jämförelser mot uppgifter i de register som förs av Migrationsverket och Skatteverket, men även av den egna myndigheten. Som exempel har nämnts att sådana behov finns för Polismyndigheten vid handlägg-

[33] RiR 2024:12, s. 85.

ning av en ansökan om en resehandling eller ett identitetskort. Vi har ovan bedömt att ett system för att verifiera identitet med hjälp av biometriska uppgifter som tar sikte på en bred krets av aktörer inte bör bygga på tillgång till befintliga register. Detta talar enligt vår uppfattning mot att inom ramen för detta betänkande överväga en ordning som innebär ett utökat informationsutbyte mellan nämnda myndigheter, i syfte att verifiera identitet med biometriska uppgifter.

Vi kan även konstatera att förslag om ett utökat informationsutbyte – som innefattar möjlighet att använda biometriska uppgifter – mellan Skatteverket och Migrationsverket har lämnats i propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten*.[34] Vidare har det i promemorian *Ett statligt identitetskort* lämnats förslag som innebär att när en person ansöker om pass eller om ett statligt identitetskort ska den ansiktsbild som tas av personen i samband med ansökan få användas för sökning i det pass- och identitetskortsregister som föreslås, i syfte att kontrollera sökandens identitet och innehav av pass eller identitetskort.[35]

När det gäller Polismyndighetens behov av att få tillgång till uppgifter hos Skatteverket för sin id-verksamhet, det vill säga vid utfärdande av pass och nationellt identitetskort, anförde Utredningen om brottsbekämpning inom Skatteverket att de utredningsförslag som avser ärenden om pass, statligt identitetskort och statlig e-legitimation syftar till att stärka identitetsförvaltningen i samhället och att föreslagna möjligheter till biometriska jämförelser i sådana ärenden kan förväntas förhindra att en enskild person samtidigt nyttjar flera pass, statliga identitetskort eller statliga e-legitimationer under skilda identiteter. Utredningen bedömde att om Polismyndigheten i sin id-verksamhet skulle få tillgång till biometriska underlag och biometriska uppgifter som lagras hos Skatteverket skulle det kunna leda till bättre identitetskontroller, men att det inte var möjligt att göra en realistisk bedömning av Polismyndighetens faktiska behov och av om en sådan tillgång skulle vara nödvändig och proportionerlig. En sådan bedömning var enligt utredningens mening beroende av bland annat vad som händer med de förslag som lämnades i betänkandet och hur Polismyndighetens id-verksamhet faktiskt kommer att se ut framöver. Bedömningen gjordes därför att frågan bör övervägas vidare i

[34] Prop. 2025/26:261, s. 77.
[35] Ju2026/01595, s. 14 f.

annat sammanhang.[36] Förslag har därefter lämnats i promemorian *Ett statligt identitetskort* och propositionen *En statlig e-legitimation*[37].

Informationsutbyte av det slag som efterfrågats för Polismyndigheten i id-verksamheten har alltså nyligen varit föremål för utredning och det finns förslag som behandlas inom Regeringskansliet såväl avseende den id-verksamheten som avseende utökad tillgång till biometriska uppgifter för Skatteverket och Migrationsverket som finns i respektive myndighets register. Detta talar som vi ser det mot att inom ramen för detta betänkande lämna sådana förslag. Vårt uppdrag går inte heller ut på att utvärdera och förbättra redan lämnade förslag. Med hänsyn till detta – och med beaktande av vår bedömning i avsnitt 10.6.1 – avser vi inte att lämna förslag som syftar till ett utökat informationsutbyte mellan Polismyndigheten, Migrationsverket och Skatteverket som bygger på tillgång till de register som dessa myndigheter för. Sådana åtgärder skulle inte heller främja en stärkt koppling mellan en etablerad identitet och verifiering av identitet i ett bredare perspektiv, på det sätt som efterfrågas i våra direktiv.

10.6.3 Utökad användning av EU-gemensamma system

Vår bedömning

En koppling mellan en av svenska myndigheter etablerad identitet och verifiering av den stärks inte genom en utökad tillgång till EU-gemensamma informationssystem. Det saknas också möjlighet att ge en bred krets av aktörer direkt tillgång till sådana system för att verifiera identitet i olika sammanhang.

Det har under vårt arbete lyfts fram att ett system för att stärka verifiering av identitet i Sverige i olika sammanhang bör kunna bygga på och inbegripa en interoperabilitet med de EU-gemensamma informationssystem som vi har redogjort för i kapitel 7. Vi anser emellertid att detta inte är ett möjligt alternativ som bör övervägas inom ramen för detta betänkande, av följande skäl.

Det omfattande arbete som pågår inom EU med att utveckla och upprätta gemensamma informationssystem och med att öka inter-

[36] SOU 2025:75, s. 536 f.
[37] Prop. 2025/26:250.

operabiliteten mellan informationssystemen, bland annat i syfte att kunna göra sökningar i flera system samtidigt bör, enligt vår mening, om möjligt dras nytta av även för att stärka svensk identitetsförvaltning och motverka identitetsmissbruk. Vi kan dock konstatera att de regelverk som styr de olika systemen är komplexa och mycket omfattande. Nationella lagstiftningsåtgärder som syftar till att utreda om anpassningar behöver ske i svensk rätt med anledning av relevanta EU-förordningar befinner sig i olika skeden, vilket bidrar till att det är svårt att ge en sammanhållen bild av hur de EU-gemensamma systemen kan och ska tillämpas. Redan dessa omständigheter talar enligt vår mening mot att direkt bygga ett nationellt system för att verifiera identitet på en interoperabilitet med dessa system. Att anpassa möjligheterna att söka i systemen ens för vissa särskilt utpekade myndigheter – i första hand Migrationsverket och Polismyndigheten – kräver i sig relativt komplexa överväganden; att utöka detta till en bred krets av svenska myndigheter och eventuellt andra aktörer framstår enligt vår mening som synnerligen komplicerat, om det ens är möjligt.

I likhet med de olika register som förs av Polismyndigheten, Migrationsverket och Skatteverket får de olika EU-gemensamma informationssystem som kan vara aktuella i detta sammanhang endast användas för särskilt angivna syften och ändamål. Till exempel framgår av artikel 9 i in- och utreseförordningen att in- och utresesystemet får användas vid gränskontroller, viseringsansökningar och inre utlänningskontroller. In- och utresförordningen – och de andra förordningar som reglerar de EU-gemensamma informationssystem som vi redogjort för i kapitel 7 – är till alla delar bindande och direkt tillämplig i alla medlemsstater, vilket betyder att den ska tillämpas direkt av nationella myndigheter på samma sätt som lagar och andra nationella föreskrifter. Det saknas alltså möjlighet att utöka tillämpningsområdet i nationell rätt, om detta inte särskilt medges i förordningen. De förordningar som styr de system som framgår av tabell 10.2 nedan saknar bestämmelser som medger att de kan användas för att i situationer av högst varierande slag verifiera identitet. I stället är det i många fall noggrant reglerat; i artikel 41.1 i gränsförordningen[38] anges exempelvis att medlemsstaterna endast får behandla uppgifter som avses i artikel 20 i syfte att neka inresa till och vistelse på deras territorier. I artikel 41.5 anges att medlemsstaters behandling av SIS-uppgifter för andra syften än de för vilka uppgifterna fördes in i Schengens in-

[38] Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018.

formationssystem (SIS) måste ha koppling till ett specifikt ärende och motiveras av behovet att avvärja en överhängande och allvarlig fara för den allmänna ordningen och säkerheten, en betydande risk för den nationella säkerheten eller ett grovt brott. En ordning som skulle tillåta att ändamålen i efterhand kan utökas väsentligt genom åtgärder i nationell rätt skulle vara svår att förena med grundläggande principer i dataskyddsförordningen.

De EU-gemensamma systemen är inte bara begränsade i fråga om syfte och ändamål, utan åtkomsten till information är i de flesta fall begränsad till vissa utpekade myndigheter vars verksamhet knyter an till de ändamål som ett visst system ska främja. Vi kan som exempel nämna artikel 6 i VIS-förordningen[39], som anger att åtkomst till VIS – det vill säga EU:s informationssystem för viseringar – är begränsad till viseringsmyndigheter, myndigheter som är behöriga att uppta eller besluta om en ansökan om visering för uppehållstillstånd och till myndigheter som ansvarar för gränskontroller och kontroller inom medlemsstaternas territorium. De svenska myndigheter som omfattas är utlandsmyndigheterna, Polismyndigheten och Migrationsverket, men även migrationsdomstolarna.[40] Merparten av de aktuella förordningarna innehåller i princip en uttömmande uppräkning av vilka typer av myndigheter som ska kunna ha åtkomst till ett visst system. I de fall det ankommer på medlemsstaterna att bestämma vilka de behöriga myndigheterna ska vara, ges en motsvarande detaljerad uppräkning i nationell rätt. Ett exempel på detta är tillgången till SIS; i 11 § förordningen (2021:1188) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem anges vilka myndigheter som ska ha åtkomst till uppgifter som förts in i SIS och rätt att söka i sådana uppgifter.

I tabellen nedan ges en sammanställning av de begränsningar i fråga om ändamål och åtkomst som vi lyft fram ovan.

[39] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008.
[40] Prop. 2024/25:176, s. 27 ff.

Tabell 10.2 Översikt över relevanta EU-gemensamma informationssystem

System	Får användas av	För följande ändamål
VIS	Utlandsmyndigheterna Polismyndigheten Migrationsverket Migrationsdomstolarna[1]	Viseringsansökningar Uppehållstillstånd Verifiering och identifiering vid gränskontroll och inre utlänningskontroll
In- och utressystemet	Utlandsmyndigheterna Polismyndigheten Migrationsverket[2]	Gränskontroller Viseringsansökningar Inre utlänningskontroller[3]
Eurodac	Migrationsverket[4] Polismyndigheten Tullverket Kustbevakningen Säkerhetspolisen Ekobrottsmyndigheten[5]	Ansökan om internationellt skydd Brottsbekämpning[6]
CIR/ESP	Polismyndigheten Myndigheter som har behörighet till underliggande system[7]	Inre utlänningskontroller Verkställighet av avlägsnandebeslut Brottsutredning[8]
Etias	Polismyndigheten Migrationsverket Säkerhetspolisen[9]	Gränskontroller Inre utlänningskontroll Ansökan om resetillstånd[10]
Ecris-TCN	Polismyndigheten[11]	Sökning i belastningsregistret
SIS	Polismyndigheten Migrationsverket Tullverket Kustbevakningen Säkerhetspolisen Åklagarmyndigheter Utlandsmyndigheterna Transportstyrelsen[12]	Gränskontroller Inre utlänningskontroller Ärenden som Migrationsverket handlägger Viseringsansökningar

[1] Artikel 6 i VIS-förordningen och prop. 2024/25:176, s. 27 ff.
[2] Artikel 9 i in- och utreseförordningen.
[3] Artikel 6, 24 och 26 i in- och utreseförordningen.
[4] 11 § förordningen (2019:502) med instruktion för Migrationsverket.
[5] 9 kap. 1 § förordningen (2017:504) om internationellt polisiärt samarbete.
[6] Artikel 32–35 i den reviderade Eurodac-förordningen.
[7] Artikel 7.1 i IOF.
[8] Artikel 20 i IOF.
[9] *Anpassning av svensk rätt till EU:s nya system för reseuppgifter och resetillstånd*, Ds 2021:19, s. 51 f.
[10] Artikel 47 och 48 i Etias-förordningen.
[11] *Nya regler om informationsutbyte om brottmålsdomar i EU*, prop. 2021/22:172, s. 36.
[12] 11 § förordningen (2021:1188) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem.

Vårt uppdrag omfattar att lämna förslag på ett system som möjliggör att fler aktörer än i dag kan få ta del av information om en etablerad identitet för att förstärka sin kontroll i verifieringssteget. Utifrån det ovan anförda är det enligt vår mening tydligt att det inte är möjligt att bygga ett sådant system på en direkt tillgång till de EU-gemensamma informationssystemen, eftersom regelverken inte medger att behöriga myndigheter eller ändamålen utvidgas i nationell rätt på det sätt som skulle krävas för en sådan lösning. Det är enligt vår bedömning inte heller möjligt att indirekt medge tillgång till systemen, exempelvis genom en nationell sökportal eller att en behörig myndighet genom en fråga-svar-funktion utför sökningar för andra aktörers räkning. Dels hindrar ändamålen som systemen får användas för detta, dels skulle det innebära en komplex och osmidig lösning.

Även om det skulle vara möjligt att ge en bredare krets av aktörer i Sverige tillgång till de uppgifter om identitet som finns i de EU-gemensamma informationssystemen skulle det – enligt vår mening – inte främja en stärkt koppling mellan en identitet som etablerats av myndigheter i Sverige och en verifiering av denna. Detta med hänsyn till att de informationssystem som framgår av tabell 10.2 ovan endast innehåller uppgifter om tredjelandsmedborgare. Sökningar i VIS avser dessutom endast personer som innehar antingen en visering eller ett uppehållstillstånd, och Eurodac innehåller endast information om personer som har ansökt om internationellt skydd. Ett nationellt system som bygger på direkta sökningar i relevanta EU-gemensamma informationssystem skulle därmed inte omfatta stora delar av den personkrets som vi – enligt våra bedömningar i kapitel 12 – anser att det finns ett behov av att verifiera identitet för. Samtidigt som personkretsen skulle vara begränsad skulle omfattningen av de personuppgifter som kan komma att behandlas att öka. Vi har i avsnitt 10.6.1 lyft fram att en utökad tillgång till de befintliga register som förs av Polismyndigheten, Migrationsverket och Skatteverket medför en sådan risk, bland annat genom att dessa register innehåller annan information om individer än de vi – enligt våra bedömningar i kapitel 11 – anser behövs i syfte att verifiera identitet biometriskt eller identifiera en person. Vi anser att motsvarande risk gör sig gällande i förhållande till de EU-gemensamma informationssystemen. Som exempel kan nämnas att en personakt i in- och utresesystemet, enligt artikel 16 i in- och utreseförordningen, ska kunna innehålla uppgifter om rese-

handlingar, datum och tidpunkt för inresa och giltighet för uppehållstillstånd och viseringar.

Vid en sammanvägd bedömning av ovanstående omständigheter anser vi att det inte är möjligt att bygga ett system – som stärker kopplingen mellan en av svenska myndigheter etablerad identitet och verifiering av den – på en utökad direkt tillgång till EU-gemensamma informationssystem för en bred krets av aktörer i Sverige.

Med detta sagt vill vi här understryka att de uppgifter om identitet som finns lagrade i EU-gemensamma informationssystem kan komma även andra myndigheter än de som framgår av tabellen ovan till godo, i syfte att stärka identitetsförvaltningen. Som vi redogjort för i avsnitt 10.6.2 finns det, och har förslagits, informationsutbyte mellan Polismyndigheten, Migrationsverket och Skatteverket. Information som de två förstnämnda myndigheterna kan inhämta från EU-gemensamma system, för att utreda och verifiera identiteten på en person som vill vistas i Sverige, i flera av de ärenden där en identitet behöver etableras i Sverige, kommer därigenom att kunna utbytas. EU-systemen kan därmed indirekt få genomslag i svensk identitetsförvaltning, även om det är begränsat till dessa tre myndigheter. Genom vår bedömning att ett identitetsindex – om ett sådant system införs – bör byggas upp utifrån de uppgifter om identitet samt biometriska underlag och biometriska uppgifter som tas fram i vissa ärendeslag (se kapitel 13) kommer information från EU-gemensamma system, enligt vår mening, indirekt att kunna komma en bred krets av aktörer till godo. På detta sätt kan befintliga *strukturer* utnyttjas, även om befintliga register och system inte används direkt.

10.7 Verifiering mot ett nytt identitetsindex

Vår bedömning

Ett system med ett identitetsindex kan stärka kopplingen mellan en etablerad identitet och verifiering av identitet med grund i biometriska uppgifter.

Med utgångspunkt i vår bedömning ovan avseende att använda befintliga register för verifiering av identitet blir frågan hur ett alternativt system för verifiering mot register skulle kunna utformas. Enligt våra

direktiv ska vi, i detta avseende, analysera det system med unika identitetsnycklar i ett identitetsindex som samverkansinitiativet MUR (Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärdssystemen) har lagt fram.[41]

Med hänsyn till de överväganden vi gör nedan i avsnitt 10.7.1–10.7.6 är vår sammantagna bedömning att ett system med ett identitetsindex kan stärka kopplingen mellan etablerad identitet och verifiering av identitet, med grund i biometriska uppgifter. Som vi belyser i avsnitt 10.7.1 finns det vissa utmaningar med ett identitetsindex. Dessa är emellertid inte i sig av det slaget att ett sådant system inte alls bör övervägas, sett till behovet av en enhetlig och sammanhållen identitetsförvaltning och den nytta som ett identitetsindex potentiellt kan medföra, inte minst på lång sikt. Det framgår, som sagt, också av våra direktiv att vi *ska* undersöka lämpligheten med ett system med en unik identitetsnyckel och analysera ett sådant system närmare; redan av denna anledning finns det skäl för utredningen att överväga hur ett sådant system skulle kunna utformas.

Med det sagt gör vi följande, inledande, överväganden avseende ett system med ett nytt identitetsindex.

10.7.1 Grunderna i ett system med ett identitetsindex och omständigheter att beakta

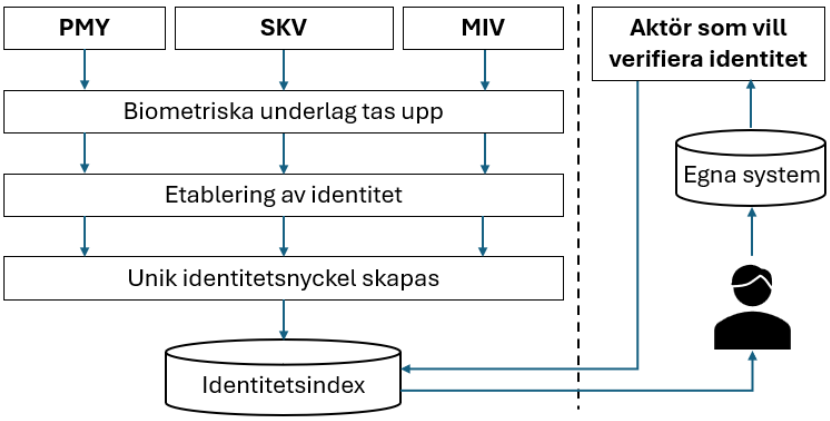
Enligt den lösningshypotes som utforskats av MUR ska en ny unik identitetskod införas, som en nyckel i ett nationellt identitetsindex. Enligt förslaget ska Skatteverket, Migrationsverket och Polismyndigheten få ta upp, lagra och ändra uppgifter om biometriska kännetecken. Dessa kännetecken ska kunna kopplas till en ny underliggande persistent identitetskod genom en numerär översättning av de referenspunkter som utläses från en fysisk person. Identitetskoden – eller identitetsnyckeln – kan, enligt lösningshypotesen, sedan användas som referensdata i utåtriktat syfte för att stärka kontroll, verifiering och autentisering av identiteter i olika situationer.

Enligt lösningshypotesen ska biometriska uppgifter alltså tas upp av Skatteverket, Migrationsverket och Polismyndigheten och därefter ligga till grund för skapandet av unika identitetsnycklar i ett gemensamt identitetsindex. Identitetsnyckeln ska sedan kunna användas

[41] Behov av en sammanhållen infrastruktur för identitet, Skatteverket, dnr 8/2765903, 2024-01-19.

även av andra myndigheter och privata aktörer i situationer där det finns ett behov av verifiering av den enskildes identitet, företrädesvis med biometriska uppgifter. Detta kan översiktligt illustreras på följande sätt.

Figur 10.1 Grunderna i ett system med ett identitetsindex



Ett system av detta slag är inte fritt från potentiella nackdelar, vilket måste beaktas. Vi kan i detta sammanhang notera att Riksrevisionen i sin rapport *Vem där – fastställande av identitet vid statliga myndigheter* bedömde att en gemensam identitetsförvaltning, med ökat fokus på biometriska uppgifter, skulle kunna bidra till en minskad risk för identitetsrelaterad brottslighet, men att det samtidigt finns en rad juridiska, integritetsmässiga, tekniska och säkerhetsmässiga hinder som innebar att myndigheten inom den då aktuella granskningen inte kunde ta ställning till hur realistisk en sådan framtida lösning skulle vara.[42] Vi vill i dessa avseenden här lyfta fram följande.

För att ett identitetsindex ska få en reell effekt i fråga om att motverka identitetsmissbruk måste det bygga på biometriska uppgifter, men även på att verifieringen kan göras med hjälp av sådana uppgifter, när ett sådant behov uppstår. Detta kommer i sin tur att förutsätta att biometriska underlag kan tas upp i fler situationer än i dag, av betydligt fler myndigheter. En sådan ordning ger naturligtvis upphov till frågor om integritetshänsyn. Sådana aspekter utgör dock, enligt vår bedömning, inte ett avgörande argument mot att i vart fall över-

[42] RiR 2024:12, s. 102.

väga att införa ett identitetsindex som utgår från en utökad användning av biometriska uppgifter, med hänsyn till att syftet i bred bemärkelse är att motverka identitetsmissbruk. I propositionen *Anpassning av svensk rätt till den reviderade VIS-förordningen* bedömde regeringen att insamlingen av biometriska uppgifter vid ansökan om nationell visering, som syftar till att minska risken för identitetsbedrägerier, uppfyller viktiga allmänna intressen.[43] Det bör även framhållas att en *möjlighet* att ta upp biometriska underlag i fler fall naturligtvis inte bör leda till att det sker regelmässigt utan att det är nödvändigt i det enskilda fallet (jfr avsnitt 21.5).

En annan integritetsaspekt som måste beaktas är att ett identitetsindex efterhand skulle innehålla biometriska uppgifter avseende ett mycket stort antal personer, merparten av dem svenska medborgare. Redan insamling och lagring av biometriska uppgifter medför risker för den personliga integriteten, och ökar riskerna för att informationen sprids till obehöriga, exempelvis vid cyberattacker. Som lyftes fram i remissyttrande från Integritetsskyddsmyndigheten över betänkandet *Biometri – för en effektivare brottsbekämpning* – där förslag bland annat lämnades om att biometriska uppgifter skulle sparas i passregistret och att Polismyndigheten, under vissa förutsättningar, skulle få göra jämförelser med dessa uppgifter – bör förslag om utökad användning av biometri också ses i ljuset av andra förslag om utökade möjligheter till användning av ansiktsigenkänning och kamerabevakning. Det är viktigt att sådana aspekter beaktas vid utformningen av såväl det rättsliga som det tekniska ramverket för ett identitetsindex.

Ett identitetsindex avser inte att ersätta de befintliga register som förs av Skatteverket, Migrationsverket eller Polismyndigheten eller andra ärendesystem som innehåller identitetsuppgifter som används av myndigheter. Detta innebär samtidigt att registrering av uppgifter om identitet och biometriska uppgifter kan komma att behöva göras både i de egna register som myndigheten har tillgång till och i ett identitetsindex. Ett identitetsindex kommer också – som vi beskriver i kapitel 14 – att behöva uppdateras, exempelvis om uppgifter om identiteten ändras genom att en person får ett nytt medborgarskap eller ändrar namn. Ett merarbete kan därmed förväntas. Att bygga upp ett identitetsindex från grunden innebär vidare att effekten och nyttan av det kan komma att dröja. Ett identitetsindex som byggs upp som ett nytt register undanröjer inte heller omedelbart de felaktigheter

[43] Prop. 2024/25:176, s. 39.

som finns i nuläget; existerande multipla och felaktiga identiteter kan komma att användas fortsättningsvis fram till att personen i fråga registreras i identitetsindexet med biometriska uppgifter. Uppbyggnad av ett nytt system kräver dessutom investeringar i infrastruktur och utveckling av nya system, anpassning av rutiner och arbetsmetoder, utbildningsinsatser hos de aktörer som kan komma att använda ett identitetsindex samt information till allmänheten. Som vi anfört i avsnitt 10.6.1 kan det, som vi ser det, emellertid antas att nyss nämnda aspekter skulle uppkomma även med ett system som bygger på befintliga register.

Ett identitetsindex kan enligt vår bedömning motverka att etablerade identiteter utnyttjas och att en individ uppträder under multipla identiteter. Genom att en digital identitet som följer individen över tid skapas i ett identitetsindex blir det svårare att byta identitet, till exempelvis för att undgå ansvar, skulder eller straff. Ett identitetsindex av detta slag kan medföra nytta på flera nivåer. (1) På individnivå kan ett identitetsindex främja att den enskilde känner sig säker på att andra inte kan uppträda i dennes identitet, genom att exempelvis använda personen som målvakt i ett bolag utan dennes vetskap. (2) På nationell nivå kan ett identitetsindex effektivt motverka användningen av kapade och multipla identiteter, exempelvis för att tillskansa sig socialförsäkringsförmåner. (3) På EU-nivå motverkas exempelvis att EES-medborgare utnyttjar rätten till fri rörlighet för personer för att etablera en identitet i Sverige som sedan kan användas av någon annan som inte vill agera i sin egen identitet.

10.7.2 Begreppet identitetsindex

Vår bedömning

Begreppet *identitetsindex* är lämpligt för att beskriva ett centralt informationssystem som innehåller unika alfanumeriska nycklar, till vilka bland annat biometriska uppgifter kopplas.

Begreppet identitetsindex förekommer bara inom ramen för den lösningshypotes som tagits fram av MUR. Med begreppet *index* avses ofta ett tal som används för att mäta och jämföra förändringar över tid, ofta i förhållande till ett basår eller en basperiod. Det kan användas

för att exempelvis följa prisutvecklingen eller aktiekurser. I it-sammanhang kan index i stället avse en datastruktur i en databas som används för att snabbt hitta poster i en tabell utan att behöva genomsöka hela tabellen varje gång. Indexet fungerar som ett ordnat register över en tabell, som gör att systemet snabbt kan lokalisera och hämta uppgifter baserat på de nycklar som definieras i indexet. Ett index kan sägas fungera som registret i en bok. Enligt den lösningshypotes som utforskats av MUR ska en ny unik identitetskod införas, som en nyckel i ett identitetsindex. Syftet med en sådan lösning är bland annat att med hjälp av en unik nyckel snabbt kunna lokalisera en individ i en databas, för att kunna hämta identitetsuppgifter och biometriska uppgifter som är kopplade till träffen. Detta motsvarar enligt vår mening i allt väsentligt vad begreppet index normalt avser i tekniska sammanhang. Att språkligt kunna särskilja ett nytt, gemensamt register från befintliga register som förs av bland annat Skatteverket, Migrationsverket och Polismyndigheten kan som vi ser det ha pedagogiska, men även lagtekniska, fördelar. Några direkta skäl som talar mot begreppet har inte kommit fram under vårt arbete. Ett index bör innehålla unika alfanumeriska nycklar till vilka bland annat uppgifter om identitet är kopplade (se kapitel 11). Vi anser mot denna bakgrund att begreppet *identitetsindex* är lämpligt för att beskriva ett nationellt informationssystem för identiteter.

10.7.3 En sammanhållen syn på information om identiteter

Vår bedömning

Ett system med ett centralt identitetsindex kan effektivt främja en sammanhållen identitetsförvaltning.

Som vi pekat på i avsnitt 10.6.1 finns det en mycket stor mängd information om identiteteter lagrad i de register som förs av Polismyndigheten, Migrationsverket och Skatteverket. Både informationen som sådan och ansvaret för den är emellertid i hög grad fragmenterat. Detsamma kan sägas för det rättsliga stödet för att i olika ärendeslag behandla identitetsuppgifter och biometriska uppgifter, vilket är svåröverskådligt och spritt över olika författningar. Sammantaget råder alltså en hög grad av fragmentering. Detta motverkas, som vi ser

det, inte av ett utökat informationsutbyte och ett sådant utbyte bör inte heller övervägas inom ramen för utredningen (se avsnitt 10.6.2). I en rapport från Skatteverket har problematiken formulerats på följande sätt.

> En genomgående utmaning är att samhällssystemet som bland annat garanterar rättigheter och skyldigheter saknar tillräcklig grad av systemövergripande, holistiskt arbetssätt där myndigheter och privata aktörer kan nyttja information, tjänster och verktyg som säkerställer att man vet vem man interagerar med.[44]

Under vårt arbete har det lyfts fram av bland annat Polismyndigheten att det finns ett behov av enkelhet. Vidare framhölls i MUR-initiativet Stärkt grundidentitet att identitetsmissbruk ofta riktar in sig mot identitetsförvaltningens svagaste länk och de som utnyttjar identiteter anpassar sig snabbt till utvecklingen. Ett robust system med helhetssyn behöver, enligt MUR, därför utvecklas.[45] Det finns alltså behov av en mer enhetlig syn på verifiering av identitet, som inte är begränsad till de åtgärder som vidtas i dessa avseenden av ovan nämnda myndigheter. Ledordet bör, enligt vår mening, vara en *sammanhållen* identitetsförvaltning. Ett centralt och gemensamt identitetsindex skulle enligt vår bedömning kunna främja detta mål, i ett längre perspektiv.

En sammanhållen identitetsförvaltning skulle bland annat effektivt motverka behovet av ett konstant informationsutbyte mellan myndigheter i fråga om verifiering av identitet. Verifiering skulle i stället kunna göras mot en central punkt. Det har bland annat i Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* lyfts fram att det saknas kompetens om id-frågor och att det behövs mer samverkan. Om ett centralt identitetsindex etableras främjas en möjlighet att samla nödvändig kompetens hos en mer begränsad krets aktörer. Ansvarsfördelning kan på samma sätt tydliggöras och uppgifter om identitet avseende en viss individ kan lagras och uppdateras på en enda plats och spridas till andra aktörer på ett mer effektivt sätt än om informationen finns lagrad i flera, myndighetsspecifika, register som förs för i huvudsak andra ändamål än att verifiera identitet. På dessa sätt finns det också förutsättningar att bättre motverka

[44] Skatteverket, *Rapport – Sammanhållen identitetsförvaltning*, den 7 april 2022.
[45] Behov av en sammanhållen infrastruktur för identitet, Skatteverket, dnr 8/2765903, 2024-01-19.

de problem som MUR-initiativet lyft fram avseende att särskilt brottsliga aktörer riktar in sig på identitetsförvaltningens ”svagaste länk”.

Ett system med ett nationellt identitetsindex, baserat på MUR:s lösningshypotes, skulle enligt vår bedömning kunna bidra till en sammanhållen identitetsförvaltning, med ökad användning av biometriska uppgifter för att koppla samman en etablerad identitet med den person som en viss aktör möter.

10.7.4 Ett identitetsindex kan främja ”en person, en identitet”

Vår bedömning

Ett system med ett centralt identitetsindex som från början bygger på biometriska uppgifter kan motverka att en individ registreras med multipla identiteter.

Ett svårlöst och återkommande problem med den nuvarande fragmenterade synen på svensk identitetsförvaltning är förekomsten av multipla identiteter. Sådana kan uppkomma inte bara genom att en enskild har flera identiteter i samma myndighets register utan också genom att han eller hon är registrerad med olika identiteter i olika myndigheters register. Möjligheten att upptäcka dessa med endast alfanumeriska sökningar får enligt vår mening anses synnerligen begränsad, och kräver manuell handläggning. I betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* konstaterades att även om Skatteverket gör ett stort antal sammankopplingar av samordningsnummer om året kan tilldelade samordningsnummer och befintliga personnummer lätt missas om de innehåller andra identitetsuppgifter än de som uppges i en anmälan, ansökan eller begäran, eller om stavningar på namn skiljer sig åt mellan registrerade och uppgivna uppgifter.[46] Detta är naturligtvis inte en ordning som främjar en tillförlitlig identitetsförvaltning.

MUR-initiativet har lyft fram att det förutsätts att biometriska uppgifter används och kopplas till identiteten för att målet med ”en person, en identitet” ska kunna uppnås.[47] Det är en förutsättning för att kunna bygga tillit, transparens och förutsägbarhet i en identitets-

[46] SOU 2025:75, s. 410 f.
[47] *Behov av en sammanhållen infrastruktur för identitet*, Skatteverket, dnr 8/2765903, 2024-01-19.

förvaltning. Vi delar denna bedömning. Som framgår av tabell 10.1 i avsnitt 10.3.2 är omfattningen av de biometriska underlag och biometriska uppgifter som får lagras och som faktiskt lagras i befintliga register i nuläget i viss mån begränsad. Förutsättningarna för att komma till rätta med multipla identiteter är därför också begränsade i ett system som bygger på dessa befintliga register. I ett centralt och gemensamt identitetsindex som utformas utifrån en unik alfanumerisk nyckel, till vilken det vid det första registreringstillfället kopplas bland annat biometriska uppgifter och identitetsuppgifter, skulle det säkerställas att endast unika identiteter registreras i systemet. Sådana problem med multipla identiteter som beror på exempelvis osäkerhet om stavningen som nämnts ovan skulle därmed undanröjas, i ett sådant system. Ett identitetsindex som innehåller endast unika identiteter, och där en viss individ kan lokaliseras genom en sökning med en unik alfanumerisk nyckel, skulle också minska behovet av en-till-många-jämförelser med biometriska uppgifter och sökningar med alfanumeriska uppgifter om identiteten, som riskerar att generera flera träffar. Detta främjar tydligt huvudsyftet med vårt uppdrag, nämligen att föreslå åtgärder som främjar en säkrare verifiering av identitet, med grund i biometriska uppgifter.

10.7.5 Många aktörer bör kunna använda systemet

Vår bedömning

Ett system med ett centralt identitetsindex bör kunna ge förutsättningar för en bred krets av aktörer att verifiera identitet, om möjligt med hjälp av biometriska uppgifter.

Polismyndigheten, Migrationsverket och Skatteverket har – som vi redogjort för i kapitel 7 och i avsnitt 10.3 – goda möjligheter att utreda och verifiera identitet och identifiera en individ, med hjälp av biometriska uppgifter, i ärenden där en grundidentitet kan behöva etableras. Vidare har ett flertal lagstiftningsåtgärder vidtagits som syftar till att öka informationsutbytet mellan dessa myndigheter. Detta är naturligtvis positivt, men tillför enligt vår mening inte några direkta möjligheter för en bredare krets aktörer i samhället att kunna verifiera identitet i olika sammanhang. Det är enligt vår mening viktigt att möj-

ligheten att använda biometriska uppgifter för att verifiera identitet – och eventuellt identifiera en person – inte är förbehållen Polismyndigheten, Migrationsverket och Skatteverket och begränsad till de ärendeslag där en grundidentitet kan behöva etableras. Identitetsmissbruk förekommer i vitt skilda delar av samhället och behovet av att verifiera identitet behöver inte heller vara kopplat till ett potentiellt identitetsmissbruk.

När det gäller statliga myndigheter kan det finnas ett behov för exempelvis Försäkringskassan och Pensionsmyndigheten att kunna verifiera identitet, om det finns anledning till det i ett enskilt ärende, även med hjälp av biometriska uppgifter. Även andra delar av samhället, till exempel socialtjänsten och hälso- och sjukvården, kan ha ett behov av att kunna verifiera en persons identitet. Polismyndigheten, Migrationsverket och Skatteverket kan också behöva verifiera identitet i andra situationer än de som beskrivits i kapitel 6; Migrationsverket har exempelvis i tidigare lagstiftningsärenden framfört att myndigheten har ett stort behov av att mer generellt kunna verifiera en utlännings identitet vid personliga kontakter med verket.[48] Andra aktörer än myndigheter kan också ha ett behov av att verifiera identitet i olika sammanhang. Ett centralt identitetsindex som bygger på unika identiteter skulle potentiellt sett kunna användas av till exempel en arbetsgivare. Många arbetsgivare gör någon form av identitetskontroll i rekryteringsprocessen, men ofta är den baserad på tillit eller utgår från en okulär kontroll av fysiska identitetshandlingar, vilka kan vara manipulerade eller utfärdade för någon annan person, vars identitet utnyttjas. En möjlighet att exempelvis jämföra en ansiktsbild som är lagrad i ett identitetsindex med den individ som intervjuas – även på distans via videokonferens – skulle kunna motverka identitetsmissbruk.

Fler aktörer har alltså behov av att få ta del av information avseende en grundidentitet som tidigare har etablerats, för att förstärka möjligheterna att verifiera identiteten i ett senare skede. Ett fristående identitetsindex – som inte är kopplat till underliggande register som förs för andra syften – skulle enligt vår bedömning ha förutsättningar att kunna användas av fler aktörer, både offentliga och privata. De rättsliga och tekniska problem som vi pekat på i avsnitt 10.6.1 gör sig, enligt vår bedömning, inte gällande på samma sätt med ett system som bygger på att uppgifter om identitet och biometriska uppgifter

[48] *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll*, SOU 2024:80, s. 508.

på förhand samlas i ett enda register, med ett begränsat och ändamålsanpassat syfte.

10.7.6 Ett identitetsindex bör byggas upp från grunden

Vår bedömning

Befintliga uppgifter om identitet samt biometriska underlag och biometriska uppgifter i de register som förs av Migrationsverket, Polismyndigheten och Skatteverket bör inte föras över till ett identitetsindex utan indexet bör byggas upp från grunden.

Vi har i avsnitt 10.6.1 bedömt att ett system för verifiering av identitet med biometriska uppgifter inte bör bygga på tillgång till befintliga register. Det skulle emellertid kunna övervägas att föra över de uppgifter om identitet samt biometriska underlag respektive uppgifter som finns lagrade i dem till ett nytt identitetsindex. Ett sådant system skulle på så sätt potentiellt komma till användning snabbare än om det byggs upp från grunden. Flera omständigheter talar emellertid mot detta.

För det första anser vi att befintliga register som förs av Polismyndigheten, Migrationsverket och Skatteverket innehåller ett förhållandevis begränsat underlag i fråga om såväl biometriska underlag som biometriska uppgifter (se tabell 10.1). När det gäller Skatteverket kan det dessutom konstateras att det i nuläget inte finns några biometriska underlag eller biometriska uppgifter registrerade i folkbokföringsverksamheten. Även med utgångspunkt i redan lagrade uppgifter skulle det därför ta viss tid innan ett identitetsindex har byggts upp, eftersom endast individer som har biometriska underlag eller biometriska uppgifter kopplade till sig bör föras över; i annat fall kan principen om ”en person, en identitet” inte upprätthållas i systemet.

För det andra innehåller befintliga register – som vi pekat på i avsitt 10.6.1 – ”överskottsinformation”, i den meningen att det inte är säkert att en individ som är registrerad i exempelvis Migrationsverkets register över fingeravtryck och fotografier också bör ingå i ett identitetsindex. Det skulle finnas svårigheter i att avgöra om uppgifterna om en viss individ bör föras över till ett identitetsindex eller inte, eftersom det inte med någon grad av säkerhet går att utreda

anledningen till att uppgifterna har registrerats i befintliga register. Under alla omständigheter skulle detta kräva manuella arbetsinsatser. Det är, enligt vår mening, viktigt att bedömningen av om någon ska registreras i ett register, oavsett slag, präglas av tydlighet och förutsebarhet. Utan en sådan kontroll riskerar behandlingen av personuppgifter i ett nytt identitetsindex att hamna i konflikt med den grundläggande princip om uppgiftsminimering som följer av artikel 5.1 i dataskyddsförordningen. Eftersom det skulle vara fråga om behandling av känsliga personuppgifter är särskild försiktighet påkallad.

Redan det ovan anförda talar, enligt vår bedömning, mot att bygga ett nytt identitetsindex på uppgifter i befintliga register. Till detta kommer att det finns brister i tillit till de befintliga registren, eftersom det är känt att det finns problem med multipla, felaktiga och falska identiteter i dem. Ett identitetsindex som bygger på befintliga register skulle därför riskera att ärva en historisk skuld av felaktigheter. Att säkerställa att dessa felaktigheter inte förs över till ett nytt index framstår som i det närmaste omöjligt och kan i vart fall antas medföra betydande arbetsinsatser. Det kan enligt vår mening ifrågasättas om det finns några reella möjligheter att genom en jämförelse mellan uppgifterna i respektive register komma åt de felaktigheter som finns. Detta med hänsyn till det mörkertal som bedöms finnas, men även till att befintliga register innehåller uppgifter om vitt skilda personkategorier. Även om multipla identiteter skulle kunna upptäckas vid en överföring till ett nytt identitetsindex skulle det vara mycket svårt att avgöra vilken av dessa identiteter som är den korrekta, om någon.

Vid en sammantagen bedömning anser vi att ett nytt identitetsindex inte bör utgå från uppgifter som finns lagrade i befintliga register som förs av Polismyndigheten, Migrationsverket och Skatteverket. Det bör i stället – på det sätt vi beskriver i kapitel 13 – byggas upp efterhand. En sådan ordning säkerställer att endast unika individer registreras i systemet. Tillförlitligheten i fråga om att kunna verifiera identitet eller identifiera en person med hjälp av biometriska uppgifter kan därmed också främjas på ett effektivt sätt.

10.8 Sammanfattande bedömning

Vår bedömning

Utredningen bör gå vidare med och utreda två huvudalternativ för att stärka kopplingen mellan en etablerad identitet och verifiering av identitet, med grund i biometriska uppgifter: ett system med ett identitetsindex respektive en möjlighet att biometriskt verifiera identitet mot handlingar.

Utredningen bör också utvärdera om myndigheter, som ett led i att kunna verifiera identitet biometriskt, bör ges en utökad möjlighet att kräva att den vars identitet ska kontrolleras inställer sig personligen.

Vi har i detta kapitel beskrivit flera tänkbara åtgärder som skulle kunna stärka kopplingen mellan en etablerad identitet och verifiering av identitet, i första hand med grund i biometriska uppgifter. Som framgår av redogörelsen finns det för- och nackdelar med respektive åtgärd.

Vi har bland annat bedömt att det, inom ramen för utredningen, inte bör övervägas att lämna förslag som tar sikte på utökade möjligheter för Polismyndigheten, Migrationsverket och Skatteverket att använda och lagra biometriska uppgifter i de ärendeslag som vi har beskrivit i kapitel 6. Vi har också bedömt att det inte är lämpligt att införa en möjlighet för andra aktörer än Polismyndigheten, Migrationsverket och Skatteverket att använda biometriska uppgifter för att jämföra dessa med sådana uppgifter i befintliga register hos dessa myndigheter samt att det inte är möjligt att bygga ett system som stärker kopplingen mellan en av svenska myndigheter etablerad identitet och verifiering av den på en utökad direkt tillgång till EU-gemensamma informationssystem för en bred krets av aktörer i Sverige.

Genomgången av tänkbara åtgärder i det här kapitlet visar, enligt vår mening, att det finns två huvudalternativ som vi bör gå vidare med och utreda, nämligen ett system med ett identitetsindex och en möjlighet – för fler aktörer och i fler situationer än vad som gäller i dag – att biometriskt verifiera identitet mot handlingar. Vi anser också att det bör utvärderas om myndigheter, som ett led i att kunna verifiera identitet biometriskt, bör ges en utökade möjligheter att kräva att den vars identitet ska kontrolleras inställer sig personligen.

Utformningen av ett system med ett identitetsindex kräver ställningstagande till ett stort antal olika delfrågor. Vi kommer i de följande kapitlen att göra överväganden i dessa avseenden och bedöma hur vissa av dessa frågor bör kunna lösas (kapitel 11–18). Detta för att konkretisera innebörden av ett sådant system och dess påverkan på bland annat den personliga integriteten. Vad gäller en möjlighet att biometriskt verifiera identitet mot handlingar kommer vi också – på motsvarande sätt – att utvärdera och åskådliggöra hur en sådan lösning bör utformas, för att fler aktörer ska kunna verifiera identitet säkert i fler situationer än i dag, samtidigt som den personliga integriteten skyddas på ett sätt som är förenligt med grundläggande rättigheter och dataskyddsförordningen (se kapitel 19 och 20). I kapitel 21 tar vi ställning till hur dessa två alternativ skulle kunna användas för att verifiera identitet, och till därmed kopplade frågor om bland annat dataskydd och skydd för den personliga integriteten.

Våra överväganden vad gäller utformningen av de två huvudalternativen kommer sedan att ligga till grund för en jämförelse av dem och en bedömning av vilket alternativ som är lämpligast för att stärka kopplingen mellan en etablerad identitet och verifiering av identitet med grund i biometriska uppgifter (se kapitel 22). Frågan om myndigheter bör ges en utökad möjlighet att, som ett led i att kunna verifiera identitet biometriskt, kräva att den vars identitet ska kontrolleras inställer sig personligen återkommer vi till först när vi tagit ställning till vilket av de två huvudalternativen som är lämpligast.

DEL 2

Två huvudalternativ

11 Uppgifter som ett identitetsindex bör innehålla

11.1 Inledning

Vi har i föregående kapitel bedömt att ett system för att stärka verifiering av identitet som bygger på ett identitetsindex är ett alternativ som bör övervägas. Ett sådant index behöver innehålla unika identiteter som bygger på en unik alfanumerisk[1] nyckel, till vilken bland annat biometriska uppgifter kopplas. I det här kapitlet redogör vi för vilka uppgifter ett sådant identitetsindex, enligt vår bedömning, behöver innehålla för att det ska kunna fylla sitt syfte.

11.2 Utgångspunkter

Det övergripande syftet med ett identitetsindex är att främja en enhetlig identitetsförvaltning, genom att samla identitetsuppgifter och biometriska uppgifter i ett gemensamt register som kan användas av en bred krets av aktörer för att verifiera identitet och, vid behov, eventuellt kunna identifiera en person. Redan namnet *identitets*index indikerar vilka typer av uppgifter som behöver finnas i det. Vi kan konstatera att det i dag finns många olika register som förs av myndigheter i Sverige, för vitt skilda ändamål, exempelvis den centrala utlänningsdatabasen, passregistret samt folkbokföringsverksamheten. Ett identitetsindex syftar inte till att ersätta dessa. Indexet behöver därför som utgångspunkt inte innehålla ärendespecifika uppgifter som kan vara registrerade i andra befintliga register; syftet med ett identitetsindex är exempelvis inte att kontrollera om någon innehar ett giltigt uppehållstillstånd utan detta framgår av den centrala

[1] Alfanumerisk innebär en kombination av både bokstäver och siffror.

utlänningsdatabasen. En minimering av antalet uppgifter kan också främja systemets tekniska funktionalitet och prestanda, och kan bidra till att hålla nere kostnaderna för lagring. Att ett identitetsindex endast bör innehålla uppgifter som behövs för att uppnå syftet med systemet ligger även i linje med den grundläggande principen om uppgiftsminimering i dataskyddsförordningen[2], som innebär att det generellt sett inte är tillåtet att samla in personuppgifter för obestämda framtida behov, endast för att de kan vara ”bra att ha”.

En annan generell utgångspunkt bör, som vi ser det, vara att ett identitetsindex inte bör innehålla uppgifter som är av sådant slag att de kan behöva uppdateras frekvent. Ett index bör inte vara kopplat till något visst ärendeslag som kan kräva att uppgifter uppdateras, till exempel om folkbokföringsadress, civilstånd, passnummer eller giltighet för ett körkort. Verifiering av identitet kräver vidare endast att uppgifter hämtas från indexet, inte att de uppdateras. För det fall att endast en eller några få myndigheter bör ansvara för att uppdatera uppgifter i ett identitetsindex bör denna arbetsbörda naturligtvis i möjligaste mån minimeras.

Ett identitetsindex utgör enligt vår bedömning ett register i traditionell mening, det vill säga att uppgifter förs in i en uppgiftssamling på ett systematiskt sätt och att de är sökbara med hjälp av vissa parametrar. Med hänsyn till den personkrets som vi anser bör kunna omfattas (se kapitel 12) kan indexet komma att innehålla uppgifter om en mycket stor mängd personer. Syftet med ett system med ett index är vidare att det ska kunna användas av många olika aktörer. Som lyftes fram i förarbetena till utlänningsdatalagen kan det vid sådana förhållanden vara lämpligt ur ett integritetsskyddsperspektiv att tydligt specificera de personuppgifter som får behandlas.[3] Vi delar denna bedömning. Det bör därför vara tydligt vilka uppgifter som ett identitetsindex bör kunna innehålla. Det måste samtidigt beaktas att ett sådant system ska kunna fungera på ett ändamålsenligt sätt över tid, och därför i viss mån måste kunna anpassas till framtida behov som kan uppstå, både av rättslig och teknisk natur. Detta kan vara svårt att förutse, vilket talar för att regleringen bör kunna innehålla viss flexibilitet. Detta kan uppnås till exempel genom att regeringen ges rätt att meddela ytterligare föreskrifter om vilka uppgifter ett identitetsindex får innehålla. Vi anser dock att det inte är en

[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[3] *Utlänningsdatalag*, prop. 2015/16:65, s. 77 f.

lämplig lösning, utan en uttömmande uppräkning i lag av vilka uppgifter som ett identitetsindex får innehålla bör användas. Anledningen till detta är utgångspunkten att endast ett begränsat antal olika typer av uppgifter bör ingå och att de bör vara av sådan art att de endast mer sällan kräver en uppdatering. Integritetshänsyn talar enligt vår mening starkt för att ändringar som avser vilka uppgifter som ett identitetsindex ska kunna innehålla kräver sådana överväganden att innehållet bör regleras i lag, inte i förordning eller föreskrifter.

Med dessa utgångspunkter gör vi följande överväganden.

11.3 Ett index bör innehålla en unik identitetsnyckel

Ett grundläggande mål med ett identitetsindex är att säkerställa att det innehåller unika individer. Det kan här erinras om att det inte är fråga om unika *identiteter*, eftersom det inte är osannolikt att flera personer har samma namn, födelsetid och medborgarskap. För att kunna lokalisera en viss unik individ vid verifiering måste de som registreras kunna särskiljas på något sätt. Det finns alltså ett behov av någon form av unik nyckel. Frågan är hur denna bör utformas. Tre möjliga alternativ beskrivs nedan.

11.3.1 En nyckel som baseras på person- eller samordningsnummer

Vår bedömning

En unik alfanumerisk nyckel bör inte baseras på ett person- eller samordningsnummer.

I Sverige förekommer två olika identitetsbeteckningar för fysiska personer: personnummer och samordningsnummer. Dessa används i många olika sammanhang i det svenska samhället, både inom den privata och den offentliga sektorn. I förarbetena till ändringar i folkbokföringslagen anfördes bland annat att personnumret är dels ett hjälpmedel för att kunna identifiera en person, dels ett sökbegrepp i olika it-system. Detsamma kan sägas för samordningsnumret.

Både personnummer och samordningsnummer är unika.[4] Det kan med hänsyn till detta framstå som naturligt att använda dessa identitetsbeteckningar som en unik alfanumerisk nyckel i ett identitetsindex. I tidigare lagstiftningsärenden har dock konstaterats att antalet personnummer är begränsat utifrån utformningen och att de inte räcker till för alla som ska ha dem.[5] Redan dessa omständigheter talar enligt vår mening mot att använda personnummer eller samordningsnummer som utgångspunkt för den unika nyckeln i ett identitetsindex. Ett personnummer innehåller dessutom information om individen genom att det går att utläsa både födelsetid och kön. Personnummer och samordningsnummer är visserligen inte känsliga personuppgifter i dataskyddsförordningens mening, men har ändå getts en särställning och får enligt 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Eftersom grundtanken är att en alfanumerisk nyckel i ett index ska kunna användas av många olika aktörer (se närmare om användningen, kapitel 18 och 21) talar integritetshänsyn, enligt vår uppfattning, mot att använda personnummer eller samordningsnummer för detta ändamål. Vid en sammantagen bedömning anser vi alltså att en alfanumerisk nyckel inte bör bygga på person- eller samordningsnummer.

11.3.2 En nyckel som baseras på biometriska underlag

Vår bedömning

En unik alfanumerisk nyckel bör inte baseras på biometriska underlag eller de biometriska uppgifter som kan tas fram ur dessa.

Enligt den lösningshypotes med ett gemensamt identitetsindex som har utforskats av samverkansinitiativet MUR (Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärdssystemen) kan en unik nyckel i ett identitetsindex baseras på en alfanumerisk översättning av de referenspunkter som utläses

[4] *Personnummer och samordningsnummer*, prop. 2008/09:111, s. 15 och 27.
[5] Prop. 2008/09:111, s. 1.

från en fysisk persons biometriska underlag och de biometriska uppgifter som kan tas fram ur det.[6] Enligt våra direktiv ska vi analysera om en sådan identitetsnyckel skulle kunna spridas tillsammans med personens identitetsbeteckning och även lagras i individens identitetshandlingar, såväl fysiska som digitala. Avsikten är att nyckeln ska kunna användas vid verifiering av identitet.

Det är tekniskt möjligt att skapa en unik alfanumerisk nyckel från biometriska uppgifter på det sätt som anges i MUR:s lösningshypotes. Den alfanumeriska koden kan i sin tur användas för att generera exempelvis en unik QR-kod.[7] Utan tekniska hjälpmedel är det vidare inte möjligt att härleda en sådan numerär kod som skapats från biometriska underlag till en viss individ. I kapitel 13 bedömer vi att registrering i ett identitetsindex bör göras endast i samband med att biometriska underlag tas upp vid handläggningen av vissa ärendeslag. En unik alfanumerisk nyckel som baseras på dessa underlag och de biometriska uppgifter som kan tas fram ur dessa kan därför framstå som en lämplig lösning.

En sådan alfanumerisk översättning av biometriska uppgifter som det skulle vara fråga om utgör emellertid i praktiken en biometrisk mall. Vi har i avsnitt 4.5 beskrivit biometriska mallar, och då bedömt att de utgör biometriska uppgifter enligt definitionen i artikel 4.14 i dataskyddsförordningen. Behandling av biometriska uppgifter för att entydigt identifiera en fysisk person utgör i sin tur behandling av så kallat känsliga personuppgifter, vilket enligt huvudregeln i artikel 9.1 i dataskyddsförordningen är förbjudet. Att sprida en alfanumerisk nyckel som baseras på biometriska uppgifter till olika aktörer, med syftet att verifiera identitet (se även avsnitt 16.4.1), skulle alltså innebära behandling av känsliga personuppgifter. Redan av det skälet skulle användningsområdet för ett index kunna bli begränsat på ett sätt som motverkar dess syfte. Användningen av en nyckel som utgör en biometrisk uppgift för att lokalisera en individ i ett identitetsindex skulle i praktiken inte heller utgöra en verifiering, utan en *identifiering*, eftersom det sker en en-till-många-jämförelse av de biometriska uppgifterna (se avsnitt 7.3). En sådan tillämpning ligger enligt vår mening inte i linje med syftet med ett system med ett identitetsindex och är inte lämplig ur integritetshänseende. En

[6] *Behov av en sammanhållen infrastruktur för identitet*, Skatteverket, dnr 8/2765903, 2024-01-19.
[7] Sajan Ambadiyila m.fl, *Biometric based Unique ID Generation and One to One Verification for Security Documents*, Procedia Computer Science 46 (2015), s. 507 ff.

regelmässig sökning med biometriska uppgifter mot hela databasen kan också innebära en betydande belastning på systemet.

För att skapa en unik alfanumerisk nyckel förutsätts inte att den baseras på unika biometriska underlag, vilket vi återkommer till i följande avsnitt. De biometriska underlagen och de biometriska uppgifter som kan tas fram ur dem är visserligen helt nödvändiga vid den tidpunkt då någon ska registreras i ett identitetsindex; en identifiering behöver – som vi återkommer till i kapitel 13 – då göras för att säkerställa att individen inte förekommer i systemet sedan tidigare med en annan identitet. De är däremot inte en förutsättning för att i ett index lokalisera den individ vars identitet ska verifieras, utan detta kan göras med hjälp av en unik alfanumerisk nyckel, eller genom en sökning med ett person- eller samordningsnummer (se avsnitt 18.3.1).

Vid en sammantagen bedömning anser vi att en unik alfanumerisk nyckel inte bör baseras på en översättning av biometriska underlag och de uppgifter som kan tas fram ur dem.

11.3.3 En identitetsnyckel baserad på ett UUID

Vår bedömning

Ett identitetsindex bör innehålla en för varje individ unik och slumpmässigt genererad alfanumerisk *identitetsnyckel*. En sådan nyckel bör vara i form av ett UUID (Universally Unique Identifier) version 4, enligt standarden RFC 9562.

Alfanumeriska nycklar av olika slag används ofta i programvara eller i databaser för att kunna identifiera ett visst unikt dataelement. Vanligt förekommande sådana unika nycklar är i form av GUID, UUID och en nyare variant, ULID. De två förstnämnda är i grunden samma sak, men UUID är den officiella standarden och används oftare i internationella sammanhang. Båda är 128-bitars identifierare som kan vara både tids- och slumpmässiga. ULID är en nyare variant, som är utformad för att kunna sorteras lexikografiskt och är tidsbaserad, vilket gör den användbar i fall där tidsordning är viktig, exempelvis i loggar. Det har enligt vår bedömning inte kommit fram omständigheter som talar för att det finns ett behov av att uppgifterna i ett

identitetsindex kan sorteras tidsmässigt. ULID bör därför inte övervägas. När det gäller GUID används det av Microsoft och definieras i deras egna specifikationer. GUID är alltså en form av UUID men används mer frekvent i Microsofts miljöer, som .NET. Ett UUID baseras på den tekniska specifikationen RFC 9562 och har en bred kompatibilitet över olika plattformar och språk. Det finns dessutom flera olika varianter som kan användas för olika ändamål. Denna form av identifierare bör därför användas.

Ett UUID kan skapas på flera sätt, beroende på programmeringsspråk och önskad version, exempelvis i Python, JavaScript, online eller genom kommandoprompten i Windows, Linux eller MacOS. Ett UUID representeras som strängar med 36 tecken, indelade i fem grupper som är separerade med bindestreck enligt följande:

609a456e-5575-413b-a76b-8016e7e5ecdc

För att ett UUID ska kunna användas som alfanumerisk nyckel i ett identitetsindex är en grundförutsättning att det är unikt. Det finns totalt 2^{122} möjliga UUID, vilket är ungefär 5.3×10^{36} möjliga kombinationer. Chansen att två likalydande UUID genereras är därför extremt liten; om man skulle generera en miljard UUID:er per sekund skulle det fortfarande behövas miljarder år innan sannolikheten för en kollision når en märkbar nivå. Med hänsyn till denna globala unikhet används UUID ofta i distribuerade system där det behöver skapas identifierare utan risk för kollisioner. Eftersom de är så unika används de ofta som primära nycklar i databaser där det inte krävs någon samordning mellan olika databasinstanser. Vi anser med hänsyn till detta att ett UUID är lämpligt att använda som en unik alfanumerisk nyckel i ett identitetsindex. Närmare bestämt bör UUID version 4 användas. Till skillnad från andra versioner som innehåller specifika komponenter som härrör från vissa indata, förlitar UUIDv4 sig enbart på slumptal för att skapa unika identifierare. Den främsta fördelen med UUIDv4 ligger i dess slumpmässighet.[8] Varje genererat UUID är statistiskt oberoende av något annat UUID, vilket gör kollisioner oerhört osannolika.

Ett UUID är varken en biometrisk uppgift eller en känslig personuppgift. Det innebär att det kan behandlas utan beaktande av de begränsningar som gäller för behandling av känsliga personuppgifter.

[8] RFC 9562, avsnitt 5.4. https://www.rfc-editor.org/rfc/rfc9562.html, senast hämtad den 15 augusti 2025

En alfanumerisk identitetsnyckel, som inte baseras på biometriska uppgifter, kan därmed spridas och användas i större utsträckning än en identitetsnyckel baserad på biometri. Dess slumpmässighet utgör i sig en integritetsskyddande aspekt.

Sammantaget anser vi att ett identitetsindex bör innehålla en, för varje individ unik och slumpmässigt genererad, alfanumerisk nyckel, i form av ett UUID, version 4. Den bör benämnas *identitetsnyckel*.

11.4 Uppgifter som bör kopplas till en identitetsnyckel

För att ett identitetsindex ska vara funktionellt och fylla sitt syfte behöver vissa uppgifter kopplas till den unika identitetsnyckel som ska kunna skapas för varje individ som registreras i systemet. Det är med hjälp av dessa uppgifter som en verifiering av identitet kan genomföras. Vi gör i dessa avseenden följande överväganden.

11.4.1 Identitetsuppgifter

Vår bedömning

Ett identitetsindex behöver innehålla uppgifter om namn, födelsetid och medborgarskap.

Med hänsyn till att syftet med ett identitetsindex är att kunna verifiera identitet i olika sammanhang är det enligt vår mening helt givet att det behöver innehålla identitetsuppgifter, det vill säga namn, födelsetid och medborgarskap, i enlighet med vår definition av begreppet i avsnitt 3.2. Sådana uppgifter lagras även regelmässigt i andra informationssystem som har som syfte att bland annat möjliggöra verifiering av identitet. Som exempel kan nämnas in- och utresesystemet, Eurodac och informationssystemet för viseringar, VIS. Med namn avses den enskildes fullständiga namn och med födelsetid menas uppgifter om år, månad och dag.

När det gäller uppgift om medborgarskap skiljer den sig mot övriga alfanumeriska uppgifter som behöver kunna kopplas till en identitetsnyckel, genom att en person kan ha flera medborgarskap

samtidigt. Exempelvis medför ett förvärv av svenskt medborgarskap genom naturalisation inte automatiskt att det tidigare medborgarskapet förloras. Frågan är om endast ett medborgarskap bör registreras i ett identitetsindex, för personer med flera medborgarskap. Vi kan notera att i folkbokföringsverksamheten registrerar Skatteverket endast det svenska medborgarskapet för den som, utöver detta, har ett eller flera utländska medborgarskap (se RÅ 2002 ref. 93). Omvänt registrerar Skatteverket att en folkbokförd person har ett eller flera utländska medborgarskap eller att personen är statslös. I den centrala utlänningsdatabasen registreras också uppgifter om medborgarskap; om en viss individ har flera kända medborgarskap registreras ett av dem som det huvudsakliga.

För den som är svensk medborgare men även har andra medborgarskap kan det – med hänsyn till att endast det svenska registreras i folkbokföringsverksamheten – framstå som lämpligt att det endast behöver finnas uppgift om ett medborgarskap knuten till en viss identitetsnyckel. Vidare registrerar Migrationsverket ett av flera kända medborgarskap som det huvudsakliga. En person som har flera medborgarskap kan dock tänkas använda olika identitetshandlingar för att legitimera sig, vilka kan ange olika medborgarskap som personen har. Han eller hon kan också tänkas uppge olika medborgarskap i olika sammanhang, och vad som för individen är det ”huvudsakliga” medborgarskapet behöver inte överensstämma med en svensk myndighets bedömning. Det är enligt vår mening därför vanskligt att peka ut ett ”huvudsakligt” medborgarskap i ett identitetsindex genom att endast *ett* medborgarskap registreras. Vid en verifiering mot ett index kan det vara av vikt att samtliga medborgarskap framgår. I annat fall kan det hända att identitetsuppgifterna inte stämmer överens. Mot denna bakgrund anser vi att samtliga – för svenska myndigheter kända – medborgarskap för en viss individ bör kunna registreras i ett identitetsindex.

11.4.2 Kön

Vår bedömning

Ett identitetsindex bör inte innehålla uppgifter om kön.

Uppgift om kön kan anses vara nära förknippad med identiteten. Exempelvis förekommer begreppet *könsidentitet* för att beteckna en persons självupplevda kön.[9] I vissa EU-förordningar på migrationsområdet omfattar begreppet identitetsuppgifter också uppgifter om kön. Som exempel kan nämnas artikel 4.13 i VIS-förordningen[10] och artikel 3.22a i in- och utreseförordningen[11]. Det kan därför övervägas om ett identitetsindex bör innehålla uppgift även om kön. Information om kön framgår emellertid indirekt redan genom ett person- eller samordningsnummer, uppgifter som vi anser att ett index bör kunna omfatta (se avsnitt 11.4.3). Det kan visserligen antas förekomma att personer som har beviljats uppehållstillstånd och ett uppehållstillståndskort med en giltighetstid om mer än ett år – och som därmed bör kunna registreras i ett identitetsindex (se avsnitt 13.3.5) – under en viss tid saknar en identitetsbeteckning; det kan tänkas att det dröjer viss tid mellan utfärdandet av uppehållstillståndskortet och att utlänningen folkbokförs i Sverige. Personen kan dessutom ha ett namn som det inte utan kännedom om ett visst land går att avgöra om det är kvinnligt eller manligt, och det förekommer även namn som används av både kvinnor och män, exempelvis Kim, Robin och Nour. I dessa fall skulle uppgift om kön kunna vara av värde för att bekräfta att personen är den som han eller hon utger sig för att vara.

Även med hänsyn till det ovan sagda kan vi konstatera att den absoluta majoriteten av de individer som kommer att registreras i ett identitetsindex kommer att ha en identitetsbeteckning. För dessa saknas ett behov av att ett identitetsindex innehåller uppgift om kön redan av den anledningen. För övriga framstår det som att behovet endast gör sig gällande i undantagsfall, som dessutom finns under en övergångstid fram till att personen folkbokförs i Sverige eller tilldelas ett samordningsnummer. Om personen är man eller kvinna kan också i de flesta fall antas framgå av den ansiktsbild som vi anser att ett index bör innehålla (se avsnitt 11.4.5). Uppgift om kön framgår även av flera av de handlingar som ofta används som underlag för verifiering av identitet, bland annat pass, nationella identitetskort och uppehållstillståndskort som utfärdas av Migrationsverket.

Mot denna bakgrund anser vi att det saknas behov av att ett identitetsindex innehåller specifika uppgifter om kön.

[9] Se bland annat *Förstärkt skydd för den personliga integriteten*, SOU 2023:37, s. 57.
[10] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008.
[11] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.

11.4.3 Person- och samordningsnummer

Vår bedömning

Ett identitetsindex bör innehålla uppgifter om personnummer och samordningsnummer.

Person- och samordningsnummer är, som vi återkommer till i avsnitt 12.3, av väsentlig betydelse för att den enskilde ska kunna agera i det svenska samhället, både i förhållande till den offentliga sektorn och till privata aktörer. I praktiken används en identitetsbeteckning ofta ensam i syfte att lokalisera en individ i ett visst system, med hänsyn till att person- och samordningsnummer är unika.[12] De kan alltså redan i dag anses fylla en funktion vid verifiering av identitet; personnummer och samordningsnummer får enligt 3 kap. 10 § dataskyddslagen behandlas utan samtycke bland annat om det är klart motiverat med hänsyn till vikten av en säker identifiering. Även om identitetsbeteckningar inte är en del av identitetsbegreppet så som vi definierat det i avsnitt 3.2 anser vi att beteckningarnas centrala funktion i det svenska samhället, i sammanhang där identiteten kontrolleras, talar för att ett identitetsindex också bör innehålla person- och samordningsnummer. Till detta kommer att de – genom att de är unika – skulle kunna användas som sökbegrepp för att lokalisera en individ i ett index, mot vilken en jämförelse av biometriska uppgifter kopplade till träffen kan göras i syfte att verifiera identitet. Att kunna använda en identitetsbeteckning som sökbegrepp bör också underlätta för den enskilde, om den alfanumeriska nyckeln inte kan användas. Omvänt kan det finnas ett värde i att kunna hämta fram ett person- eller samordningsnummer som är kopplat till en viss individ i ett identitetsindex genom en identifiering med hjälp av biometriska uppgifter. Ett personnummer eller samordningsnummer är också bestående, på ett sätt som motverkar att en uppdatering av uppgifterna i ett index behöver ske frekvent.

Vid en sammantagen bedömning av dessa omständigheter anser vi att det finns behov av att ett identitetsindex innehåller uppgifter om personnummer och samordningsnummer.

[12] Prop. 2008/09:111, s. 15 och 27.

11.4.4 Migrationsverkets individnummer

Vår bedömning

Ett identitetsindex bör innehålla uppgifter om ett sådant individnummer som Migrationsverket registrerar.

Vi har inledningsvis bedömt att utgångspunkten bör vara att ett identitetsindex inte ska innehålla ärendespecifika uppgifter som är registrerade i andra befintliga register, exempelvis vägtrafikregistret eller passregistret. Det skulle visserligen kunna vara av värde att direkt vid en verifiering mot ett index få tillgång även till vissa vanligen förekommande uppgifter som kan vara användbara, exempelvis om folkbokföringsadress, nummer på passhandling eller körkort, eller om en person vistas i landet med ett giltigt uppehållstillstånd. Sådana uppgifter kan dock, med hjälp av de identitetsuppgifter som tas fram vid verifieringen, hämtas från det aktuella ärendesystem som den myndighet som kontrollerar identiteten förfogar över, om detta är nödvändigt. Denna typ av ärendespecifika uppgifter kan också antas behöva uppdateras med viss regelbundenhet, vilket ytterligare talar mot att ett identitetsindex bör innehålla sådana uppgifter.

Med detta sagt anser vi att avsteg från denna princip kan övervägas när det gäller sådana individnummer som Migrationsverket registrerar för personer som har ett ärende hos myndigheten, exempelvis vid en ansökan om uppehållstillstånd. Det har tidigare benämnts dossiernummer. När en person för första gången blir aktuell i ett ärende hos Migrationsverket läggs en ny dossier upp. I denna dossier samlas sedan alla uppgifter i ärendet och, om det är aktuellt, senare ärenden som rör personen. Individnumret består av en sifferkombination och är unikt. Det följer som sagt en individ även i framtida ärenden.

Migrationsverkets individnummer skulle som vi ser det kunna ha ett värde i ett identitetsindex för de personer som kommer att sakna en identitetsbeteckning i samband med registreringen. Med utgångspunkt i våra bedömningar avseende vilka personkategorier som bör omfattas av ett identitetsindex (kapitel 12) och när en identitetsnyckel bör skapas (kapitel 13) kan vi konstatera att det endast skulle vara fråga om en mycket begränsad krets av personer, nämligen de som har fått ett uppehållstillståndskort utfärdat men ännu inte

blivit folkbokförda eller tilldelats ett samordningsnummer. Det är dessutom normalt sett fråga om en övergående situation; personer som har beviljats uppehållstillstånd i mer än ett år ska som huvudregel folkbokföras i landet. Vi kan dock konstatera att det inte går att säkerställa att en person som fått ett uppehållstillståndskort utfärdat också folkbokförs, eftersom folkbokföring förutsätter en anmälan från den enskilde.

Även med beaktande av det ovan sagda anser vi att det är viktigt att denna grupp kan fångas upp av ett identitetsindex under den period en identitetsbeteckning eventuellt saknas, inte minst med hänsyn till att Migrationsverkets individnummer skulle kunna användas för att lokalisera en person i ett index (se avsnitt 18.3.1). Av information för asylsökande på Migrationsverkets hemsida framgår att vid kontakt med Migrationsverket kan information om en ansökan tas fram med hjälp av individnumret.[13] Det kan då vara av värde att med hjälp av samma unika nummer lokalisera en person i ett identitetsindex. Individnumret är, till skillnad från ett person- eller samordningsnummer, inte heller av särskild skyddsvärd art i dataskyddshänseende. Det används även för att identifiera utländska medborgare i ärenden hos Polismyndigheten och i migrationsdomstolarna. I syfte att främja en möjlighet att följa en individ vid kontakt med olika myndigheter i Sverige anser vi därför att det kan vara en fördel att även Migrationsverkets individnummer kan lagras i ett identitetsindex. En sådan möjlighet skulle även kunna motverka de problem med att multipla identiteter registreras hos Migrationsverket som vi redogjort för i avsnitt 9.2.3. Individnumret är bestående på ett sätt som motverkar att en uppdatering av sådana uppgifter i ett index behöver ske frekvent.

Sammantaget anser vi alltså att det finns ett behov av att ett identitetsindex innehåller uppgifter om sådana individnummer som Migrationsverket registrerar.

[13] https://www.migrationsverket.se/du-vantar-pa-beslut/asyl/du-har-ansokt-om-asyl/lma-kort.html, hämtad den 18 maj 2026.

11.4.5 Biometriska underlag och biometriska uppgifter

Vår bedömning

Ett identitetsindex bör innehålla ansiktsbilder och de biometriska uppgifter som kan tas fram ur dessa. Fingeravtryck och de biometriska uppgifter som kan tas fram ur dem bör däremot *inte* lagras i ett identitetsindex.

Med biometriska underlag avses en persons fysiska kännetecken. De underlag som i första hand används för verifiering av identitet och identifiering av personer i de sammanhang som är aktuella utifrån vårt uppdrag är fingeravtryck och ansiktsbilder. Användningen av dessa underlag och de biometriska uppgifter som kan tas fram ur dem är väl beprövad, och de används exempelvis i passhandlingar. Vidare finns det utrustning och processer för hanteringen av ansiktsbilder och fingeravtryck hos Polismyndigheten, Migrationsverket och Skatteverket. Det är också den typ av biometriska underlag som det finns ett rättsligt stöd för att ta upp i olika sammanhang (se kapitel 13). Vi kommer därför att begränsa våra överväganden till dessa biometriska underlag. Ur de biometriska underlagen kan biometriska uppgifter tas fram. Det är dessa uppgifter som används för den biometriska jämförelsen som görs för att koppla de uppgifter om identitet som utgör jämförelseunderlaget till individen (se avsnitt 7.2.1). Frågan är vilka av dessa typer av uppgifter som ett identitetsindex bör innehålla.

Biometriska underlag i form av ansiktsbilder

Biometriska underlag i form av ansiktsbilder lagras redan i dag i exempelvis den centrala utlänningsdatabasen, passregistret och Polismyndighetens digitala ärendehanteringssystem för handläggning av ärenden om pass och nationella identitetskort (RES). I betänkandet *Ett säkert statligt ID-kort – med e-legitimation* lyftes bland annat fram att en manuell, okulär jämförelse av ansiktsbilder fyller en viktig roll i den identitetskontroll som görs i samband med utfärdande av identitetshandlingar.[14] Detta har enligt vår mening bäring även i de samman-

[14] SOU 2019:14, s. 293.

hang som ett identitetsindex kan komma att användas. En ordning där en ansiktsbild lagras i ett index och kan användas för att okulärt jämföras med den individ vars identitet behöver verifieras, i fall där en biometrisk jämförelse inte är möjlig eller lämplig, skulle enligt vår bedömning medföra en säkrare och snabbare handläggning vid många identitetskontroller.

Att endast använda en okulär jämförelse med en ansiktsbild är inte en lika tillförlitlig metod vid verifiering av identitet som användning av biometriska uppgifter. Vi anser emellertid att möjligheten att göra en jämförelse med en ansiktsbild kan tjäna en viktig roll i att minska risken för att en enskild utnyttjar en annan persons identitet eller uppträder som en annan person. Kopplingen mellan individen som en myndighet eller annan aktör möter och det jämförelseunderlag i fråga om identitetsuppgifter som är registrerat för personen i ett index skulle stärkas om en kontroll mot en ansiktsbild är möjlig. En fördel är vidare att en okulär jämförelse skulle kunna göras på distans. Ett tänkbart exempel kan vara att en arbetsgivare genomför en anställningsintervju via videosamtal och då, genom att direkt jämföra intervjupersonen med den ansiktsbild som är lagrad i ett identitetsindex, kan använda dessa uppgifter för att verifiera att personen är den som han eller hon utger sig för att vara (se kapitel 18 och 21 för våra överväganden avseende hur ett index bör kunna användas).

Under alla omständigheter bör en möjlighet att använda ansiktsbilder i viss utsträckning kunna verka avskräckande. En okulär jämförelse mot en lagrad ansiktsbild kan också tjäna som en kompletterande utredningsåtgärd även i de fall en biometrisk verifiering genomförs; 2017 års ID-kortsutredning pekade på att även om det i dag finns program för ansiktsigenkänning som har mycket hög träffsäkerhet kan ett förändrat utseende på grund av åldrande eller sjukdom göra att en person av det automatiska systemet felaktigt klassificeras som två olika personer.[15] Vi ser inte anledning att ha en annan uppfattning.

Något som talar mot ett behov av att lagra ansiktsbilder är att en individ många gånger legitimerar sig med hjälp av en fysisk identitetshandling, som innehåller ett fotografi. I sådana fall får en jämförelse även mot den ansiktsbild som finns lagrad i ett identitetsindex anses tillföra relativt liten nytta för att verifiera identiteten. Även den omständigheten att en ansiktsbild kan behöva uppdateras med vissa

[15] SOU 2019:14, s. 298.

intervaller för att vara användbar som jämförelsematerial talar i viss mån mot att ett identitetsindex behöver innehålla sådana uppgifter. I synnerhet kan nyttan antas vara begränsad för barn som är små. Detta med hänsyn till att den fysiska utveckling som yngre barn genomgår gör att en lagrad ansiktsbild efter kort tid kan bli inaktuell. Detta har pekats på av bland annat Utredningen om brottsbekämpning inom Skatteverket, som emellertid bedömde att det inte fanns anledning att undanta yngre barn från förslagen om möjlighet för Skatteverket att lagra biometriska underlag i form av ansiktsbild i folkbokföringsverksamheten. Vid bedömningen beaktades bland annat att det inte går att bortse från möjligheten att den tekniska utvecklingen gör att det i en inte avlägsen framtid går att använda ansiktsbilder under betydligt längre tid än i dag.[16] Något som ger anledning att här göra en annan bedömning har inte kommit fram. Till detta kommer att ett identitetsindex, i enlighet med vår bedömning i avsnitt 12.4.1, bör omfatta endast personer som har fyllt sex år. Vid den åldern kan en ansiktsbild antas ha ett värde som jämförelsematerial vid verifiering av identitet.

Även om ett identitetsindex ska bygga på verifiering med hjälp av biometriska uppgifter anser vi att syftet med ett index – särskilt i situationer då biometrisk verifiering av identitet inte kan användas – främjas genom att det innehåller biometriska underlag i form av ansiktsbilder. Det bör därför innehålla sådana uppgifter.

Biometriska uppgifter som kan tas fram ur en ansiktsbild

Enligt våra direktiv ska vi lämna förslag som stärker kopplingen mellan fastställd identitet och verifiering av identitet med grund i biometriska uppgifter. För att främja detta mål och för att syftet med ett index ska kunna uppnås är det därför givet att det behöver innehålla biometriska uppgifter. Vi har särskilt beaktat följande.

En verifiering av identitet som görs med hjälp av biometriska underlag kräver som utgångspunkt en manuell analys, och är beroende av utbildning och kunskap hos den person som gör jämförelsen, och till viss del dennes subjektiva bedömning. Att identifiera en person med en sådan jämförelse av ansiktsbilder i en databas av den omfattning som ett identitetsindex kan antas få framstår enligt vår

[16] *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 426.

mening i praktiken som omöjligt. Även verifiering av identitet med hjälp av biometriska underlag, det vill säga en en-till-en-jämförelse, tar viss tid i anspråk och är inte en objektiv eller helt tillförlitlig jämförelsemetod. Det är i stället de biometriska uppgifter som kan tas fram ur en ansiktsbild som används för biometrisk verifiering av identitet och identifiering. Detta framgår till exempel av definitionen av biometrisk verifiering i artikel 3.36 i AI-förordningen[17] som anger att med detta begrepp avses ”automatiserad en-till-en-verifiering, inklusive autentisering, av fysiska personers identitet genom jämförelse av deras biometriska uppgifter med tidigare lämnade biometriska uppgifter.” Att det är de biometriska uppgifterna som används för verifieringen framgår också indirekt av definitionen av biometriska uppgifter i artikel 4.14 i dataskyddsförordningen; enligt ordalydelsen är det de biometriska uppgifterna som möjliggör eller bekräftar identifieringen av den fysiska person som underlaget, såsom ansiktsbilder eller fingeravtryck, har tagits upp av.

För att syftet med ett identitetsindex ska kunna uppnås förutsätts enligt vår mening att datorstödda jämförelser av biometriska uppgifter med hjälp av dataalgoritmer, inte en manuell granskning, kan genomföras. Att biometriska uppgifter är en förutsättning för automatiska jämförelser har lyfts fram bland annat av Biometriutredningen i fråga om möjligheten att jämföra ansiktsbilder av oidentifierade gärningsmän med ansiktsbilder i passregistret.[18] Detta utesluter emellertid inte att även sådana okulära jämförelser av ansiktsbilder som vi redogjort för ovan har ett värde för att främja en stärkt koppling mellan en etablerad identitet och verifiering av identitet. Att urvalet ska kunna ske genom datorstödda jämförelser av biometriska uppgifter betyder inte heller att en manuell granskning inte i vissa fall kan behöva göras av resultatet av en sökning. Utredningen om brottsbekämpning inom Skatteverket utgick exempelvis från att automatiserade biometriska jämförelser vid en identitetskontroll förutsätter att en manuell kontroll av träffresultatet utförs av en handläggare i efterhand.[19]

Det ska i detta sammanhang lyftas fram att vi inte ser det som ett alternativ att de biometriska uppgifterna tas fram ur underlag som lagrats i ett identitetsindex vid varje tillfälle, dynamiskt, när en

[17] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024.
[18] *Biometri – för en effektivare brottsbekämpning*, SOU 2023:32, s. 448.
[19] SOU 2025:75, s. 560.

jämförelse ska göras. Även om det skulle vara möjligt att göra detta med bibehållen prestanda vid en verifiering mot en viss träff skulle det leda till betydande prestandaförluster vid en identifiering. Biometriutredningen bedömde i fråga om vägtrafikregistret att en sådan teknisk lösning skulle innebära att registret inte kan användas för andra ändamål under tiden identifiering genomförs.[20] Motsvarande skulle enligt vår bedömning gälla för ett identitetsindex. I avsnitt 13.2.1 bedömer vi att en identifiering behöver göras innan en identitetsnyckel skapas, eftersom det är helt avgörande för att endast unika individer ska registreras. De biometriska uppgifterna för samtliga individer i systemet skulle med en dynamisk lösning då behöva genereras vid varje sådant tillfälle, vilket i praktiken skulle omöjliggöra en sådan kontroll.

De biometriska uppgifterna innehåller de särdrag som kan extraheras från biometriska underlag. För att möjliggöra en snabb och effektiv jämförelse används emellertid ofta vad som benämns biometriska *mallar*. Till exempel ska den gemensamma biometriska matchningstjänst som införs genom EU:s interoperabilitetsförordningar[21] bygga helt på biometriska mallar, som skapas ur biometriska uppgifter för en individ som kan finnas lagrade i ett annat system, bland annat Eurodac och VIS. Som vi redogjort för i avsnitt 4.5 är en biometrisk mall inte en egen rättslig figur utan en sådan mall är per definition biometriska uppgifter; en biometrisk mall utgör en teknisk, eventuell ytterligare, abstraktion av de biometriska uppgifterna för att möjliggöra snabbare och effektivare jämförelser med hjälp av en algoritm. Det krävs därmed inte att det särskilt anges att ett identitetsindex bör innehålla biometriska mallar utan det täcks redan av att ett index, enligt den bedömning vi gör nedan, bör innehålla biometriska uppgifter. Vi kan i detta sammanhang konstatera att biometriska mallar har flera fördelar. För det första innehåller de endast de mest relevanta och igenkännbara biometriska kännetecknen. Färre datapunkter medför att filstorleken för mallen kan vara mindre, vilket i sin tur ställer lägre krav på lagring, bandbredd och resurser för att bearbeta uppgifterna. Detta kan påverka prestanda, särskilt i realtidstillämpningar. Eftersom mallen utgör en ytterligare matematisk bearbetning och abstrahering av de biometriska uppgifterna främjas

[20] SOU 2023:32, s. 477.
[21] Europaparlamentets och rådets förordningar (EU) 2019/817 och (EU) 2019/818 av den 20 maj 2019.

ett skydd mot att uppgifterna omvandlas tillbaka till det ursprungliga underlaget, för det fall mallen skulle spridas till obehöriga aktörer.

Mot denna bakgrund anser vi att det finns ett mycket tydligt behov av att ett identitetsindex innehåller biometriska uppgifter som kan tas fram ur en ansiktsbild. Att endast använda de biometriska underlagen är inte ett alternativ, inte minst då detta skulle omöjliggöra att ett index används för identifiering av en individ. Att ett index innehåller biometriska uppgifter är också en förutsättning för att biometrisk verifiering ska kunna genomföras på ett effektivt och snabbt sätt, vilket är huvudsyftet med ett sådant system.

Fingeravtryck och biometriska uppgifter som kan tas fram ur dem

Frågan är om även fingeravtryck och/eller de biometriska uppgifter som kan tas fram ur dem bör få lagras i ett identitetsindex. Fingeravtryck tas i flera av de ärendeslag där en grundidentitet etableras, exempelvis med stöd av 9 kap. 8 § utlänningslagen (2005:716) och 26 c § folkbokföringslagen (1991:481). Fingeravtryck tas också exempelvis i samband med en ansökan om pass, med stöd av 6 § passlagen (1978:302). Det skulle därför som utgångspunkt kunna vara möjligt att lagra också den typen av underlag och biometriska uppgifter i ett identitetsindex. Med hänsyn till den grundläggande principen om uppgiftsminimering i dataskyddsförordningen bör det enligt vår bedömning emellertid övervägas om det är tillräckligt att ett index innehåller ansiktsbilder och de biometriska uppgifter som kan tas fram ur dem. Liknande överväganden gjordes i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning*, där följande anfördes.

> Utredningen bedömer, inte minst mot bakgrund av uppgifterna från NFC, att det i de flesta fall kan antas vara tillräckligt att jämföra underlagen av endera en ansiktsbild eller ett fingeravtryck för att verifiera en enskilds identitet. Det står ändå klart att en kontroll av flera typer av biometriska uppgifter i åtskilliga situationer skulle ge en större säkerhet än vad som skulle vara fallet om underlaget var mer begränsat. Vidare ger en rätt för kontrollerande myndighet att välja vilket biometriskt underlag som ska registreras möjlighet till anpassning efter varje enskilt fall. Behov av sådan anpassning kan vara nödvändig t.ex. när den som

> ska kontrolleras har allvarliga skador i ansikte eller på händerna eller om tekniska problem inte möjliggör åtkomst till ett visst lagrat underlag.[22]

Det har under vårt arbete inte kommit fram omständigheter som ger anledning att ha någon annan uppfattning i dessa avseenden. Även om principen om uppgiftsminimering ska beaktas bör behovet av att ett identitetsindex kan fungera på det sätt som avses prioriteras i detta sammanhang. En viktig del i detta är enligt vår mening att möjliggöra en robust jämförelsemekanism som kan användas i så många situationer som möjligt, under varierande förhållanden. Att använda två olika typer av biometriska underlag och uppgifter för att verifiera identitet innebär en ökad säkerhet jämfört med om bara en typ används. Det gör också att det finns fler valmöjligheter när det gäller teknik för verifiering av identitet. Möjligheten att verifiera identitet med hjälp av biometriska uppgifter vid ett visst givet tillfälle bör inte i praktiken vara avhängig exempelvis av om utrustning för att ta upp antingen fingeravtryck eller ansiktsbild är ur funktion. En möjlighet att lagra även fingeravtryck och biometriska uppgifter som kan tas fram ur dessa skulle kunna utgöra en betydelsefull del i att motverka sådana begränsningar. Det måste även beaktas att målet med ett identitetsindex är att det ska kunna användas av en bred skara aktörer i samhället. Dessa kan ha olika förutsättningar för att ta upp biometriska underlag av det ena eller andra slaget.

Att jämföra biometriska *underlag* i form av fingeravtryck okulärt, på det sätt som är möjligt för en ansiktsbild, är enligt vår bedömning emellertid mycket svårt. En jämförelse av underlag i form av fingeravtryck görs genom standardiserade metoder som kräver särskilda kunskaper och ett systematiskt och strukturerat tillvägagångssätt för att analysera och utvärdera information om detaljer i avtrycket.[23] Den aktör som vill verifiera en persons identitet med hjälp av biometriska uppgifter som är lagrade i ett identitetsindex kommer normalt inte att ha möjlighet att göra en sådan jämförelse av fingeravtryck. Detta talar enligt vår mening starkt mot att ett index även bör innehålla biometriska underlag i form av fingeravtryck; det skulle inte heller ge några ytterligare möjligheter att verifiera identitet på distans eller i de fall biometrisk verifiering inte kan eller får användas, på det sätt som är möjligt för ansiktsbilder. Det är – som vi lyft fram ovan – ur prestandasynpunkt inte möjligt eller lämpligt att ta fram

[22] SOU 2025:75, s. 424.
[23] SOU 2023:32, s. 220.

de biometriska uppgifter som behövs för verifiering eller identifiering i samband med att en sökning görs mot ett identitetsindex. Det finns därför inte heller av den anledningen behov av att lagra biometriska underlag i form av fingeravtryck.

En möjlighet att verifiera identitet med hjälp av båda typer av biometriska uppgifter skulle visserligen kunna ha fördelar, genom att det bidrar till en redundans och att olika aktörer kan välja den metod som är lämpligast i det enskilda fallet. Vi anser dock att det saknas stöd för slutsatsen att användning av endast ansiktsbilder och de biometriska uppgifter som kan tas fram ur dessa skulle påverka systemets användbarhet på ett negativt sätt, annat än i undantagsfall; som vi pekat på ovan bedömde Utredningen om brottsbekämpning inom Skatteverket att det i de flesta fall kan antas vara tillräckligt att jämföra underlagen av endera en ansiktsbild eller ett fingeravtryck för att verifiera en enskilds identitet.

Sammantaget anser vi att det inte finns ett utpräglat behov av att även fingeravtryck och de biometriska uppgifter som kan tas fram ur dem behandlas i ett identitetsindex. Det har under vårt arbete inte heller kommit fram omständigheter som visar på att risken för angrepp mot ett sådant jämförelsematerial skulle vara betydligt mindre än för ansiktsbilder, och att fingeravtryck därför också behöver lagras för att motverka detta. Angrepp mot fingeravtrycksigenkänning kan exempelvis ske genom att gelatinavgjutningar av fingeravtryck och digitalt utskrivna fingeravtryck används, eller genom att personen blåser på en sensor för att återanvända latenta fingeravtryck.[24] Vid ansiktsigenkänning kan bland annat tänkas att utskrivna foton av ett ansikte visas för kameran eller att personen har på sig en mask. Under förutsättning att de biometriska underlagen tas upp vid personlig inställelse i samband med att verifieringen ska genomföras kan det, enligt vår mening, emellertid antas vara mycket sällsynt att angrepp av det slag som nyss nämnts kan användas med framgång. Säkerhetsaspekter visar därmed, enligt vår mening, inte på ett behov av att lagra även fingeravtryck i ett identitetsindex.

Att lagra även biometriska underlag i form av fingeravtryck och de biometriska uppgifter som kan tas fram ur dessa skulle medföra behandling av ytterligare en typ av biometriska underlag och biometriska uppgifter för en potentiellt stor mängd personer. Integritetshänsyn förutsätter därför att det finns mycket tydliga behov som

[24] FOI, rapport från januari 2021, *Biometriska metoder för teknisk bevakning*, s. 28.

medför att syftet med ett index och dess användning främjas. Vi anser, med hänsyn till de omständigheter som anförts ovan, att ett sådant tydligt behov saknas. Vi kan i detta sammanhang även konstatera att i vissa av de ärendeslag där fingeravtryck tas upp – exempelvis vid en ansökan om pass – har lagring av fingeravtrycken uttryckligen begränsats, av integritetshänsyn.[25]

Vid en sammanvägd bedömning av dessa omständigheter anser vi att fingeravtryck och sådana biometriska uppgifter som kan tas fram ur dem inte bör lagras i ett identitetsindex.

11.4.6 Särskilt om sekretessmarkering

Vår bedömning

Ett identitetsindex bör innehålla en notering om att en viss individ har en sekretessmarkering i folkbokföringen.

En person som är utsatt för våld eller hot kan få skyddade personuppgifter i fråga om bland annat namn och adress i folkbokföringsverksamheten. Det finns tre olika typer av skydd: *skyddad folkbokföring*, som innebär att personen blir folkbokförd på en annan folkbokföringsort än den där han eller hon bor, *sekretessmarkering*, som fungerar som en varningssignal innan uppgifterna lämnas ut och *fingerade personuppgifter*, vilket innebär att en person får ett nytt namn och nytt personnummer. I ett identitetsindex kommer uppgifter om adress inte att behandlas. Något särskilt skydd i ett index för denna uppgift behövs därför inte enligt vår bedömning. Om en person har en sekretessmarkering i folkbokföringen avseende namn kan detta emellertid behöva noteras även i ett identitetsindex.

Sekretessmarkering är den minst ingripande formen av skyddade personuppgifter. En sekretessmarkering i folkbokföringen är endast en anteckning som innebär att det kan antas att en uppgift i en allmän handling inte får lämnas ut på grund av en bestämmelse om sekretess. Detta följer av 2 kap. 20 tryckfrihetsförordningen och 5 kap. 5 § offentlighets- och sekretesslagen (2009:400). Om handlingen är elektronisk får markeringen göras i det datasystem där den elek-

[25] Jfr promemorian *Ett statligt identitetskort*, Ju2026/01595, s. 130 ff., *Passdatalag*, Ds 2019:5, s. 148 och *Fingeravtryck i pass*, prop. 2008/09:132, s. 12 f.

troniska handlingen hanteras. Anteckningen ska ange tillämplig sekretessbestämmelse, datum då anteckningen gjordes, och den myndighet som har gjort anteckningen. Skatteverkets beslut om sekretessmarkering av uppgifter i folkbokföringen är en administrativ åtgärd som i sig saknar rättsverkningar. Högsta förvaltningsdomstolen har bedömt att myndighetens beslut inte är överklagbara (jfr RÅ 2005 ref. 12 och RÅ 2006 ref. 61). Markeringen innebär att Skatteverket, och andra myndigheter som hämtar uppgifter från folkbokföringsverksamheten, får en signal om att det kan finnas bestämmelser om sekretess som behöver tillämpas. En myndighet som använder Navet[26] får en signal när en person har en sekretessmarkering och uppmärksammas därmed på att de uppgifter som hämtas kan vara sekretessbelagda. Det är sedan upp till den myndigheten att göra en noggrann sekretessprövning i det enskilda fallet om det blir aktuellt. När det gäller distribution av uppgifter till allmänheten sker detta genom Statens personadressregister, SPAR. En sekretessmarkering i folkbokföringen medför att uppgifter om den berörda personens namn och adress tas bort från SPAR; personnumret är emellertid fortfarande synligt.[27]

Det är av stor vikt att det vid utlämnande av uppgifter om en viss individ i ett identitetsindex uppmärksammas om han eller hon omfattas av en sekretessmarkering i folkbokföringen. Ett index bör därför också kunna innehålla uppgift om en sekretessmarkering. Något särskilt rättsligt stöd för detta krävs inte, utöver de bestämmelser som angetts ovan. Vi anser dock att det av tydlighetsskäl bör anges uttryckligen att ett identitetsindex bör kunna innehålla en sådan anteckning. Markeringen är, som vi ser det, inte i sig en särskild personuppgift som behandlas för en viss individ utan ska, på samma sätt som i folkbokföringsverksamheten, fungera som en administrativ åtgärd i systemet. En sekretessmarkering behöver kunna föras in i ett index när en identitetsnyckel skapas (se avsnitt 13.2.2) och när en sådan markering förs in eller tas bort i folkbokföringsverksamheten av Skatteverket bör ett identitetsindex uppdateras på motsvarande sätt (se avsnitt 14.3.3).

Det bör här påpekas att det inte bör markeras i ett index om personen har skyddad folkbokföring. Eftersom uppgift om adress inte kommer att behandlas i ett index tillför en sådan markering inget.

[26] Skatteverkets system för distribution av folkbokföringsuppgifter till samhället.
[27] Jfr *Ökad trygghet för hotade och förföljda personer*, SOU 2015:69, s. 243 och Skatteverket, *Vägledning för hantering av skyddade personuppgifter*.

12 Personkategorier som bör omfattas

12.1 Inledning

En naturlig utgångspunkt för att ett system för att verifiera identitet ska kunna få så stor nytta som möjligt är att en bred krets av personer kan omfattas. Hur personkretsen bör avgränsas ska vi enligt våra direktiv särskilt analysera. Detta innefattar i huvudsak en analys av vilka personkategorier som det finns ett behov av att inkludera, och vilka personer som bör och kan omfattas. Det senare kräver bland annat ställningstaganden om dataskydd och personlig integritet, inte minst den grundläggande principen om uppgiftsminimering i dataskyddsförordningen[1], som innebär att fler personuppgifter än vad som behövs inte ska behandlas; det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov, för att de kan vara ”bra att ha”. I detta kapitel redogör vi för vilka behov det finns av att låta ett system för att biometriskt verifiera identitet omfatta olika personkategorier.

12.2 Utgångspunkter

Det huvudsakliga syftet med ett system som stärker kopplingen mellan en grundidentitet och verifiering av identitet är att det ska kunna användas för att bekräfta att en person som en myndighet eller någon annan aktör i samhället möter är den som han eller hon utger sig för att vara. Utgångspunkten för vilka personkategorier som bör omfattas av en sådan möjlighet är därför att den bör kunna omfatta alla personer som av olika anledningar kan antas agera i det

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

svenska samhället. Att detta kan omfatta ett stort antal människor framstår som självklart. Alla har emellertid inte lika stark koppling till Sverige, vilket kan påverka behovet av att kunna biometriskt verifiera deras identitet. Begrepp som används i olika rättsliga sammanhang för att beskriva en koppling till Sverige är exempelvis att någon har en *anknytning* till Sverige, att han eller hon anses *bosatt* i landet eller har *hemvist* här. Dessa begrepp beskrivs nedan. Ju starkare koppling en person har till landet, desto större behov kan det också antas finnas av att kunna verifiera personens identitet biometriskt med hjälp av något av de system som vi anser bör övervägas. Samtidigt kan det finnas personer som trots en stark anknytning inte behöver omfattas. Överväganden avseende vilka kategorier som enligt vår mening inte behöver omfattas finns avsnitt 12.4.

12.2.1 Hemvist i Sverige

Hemvist är ett internationellt vedertaget begrepp som används inom många rättsområden. Innebörden av begreppet skiljer sig dock åt. En legaldefinition finns i svensk rätt i 7 kap. 2 § lagen (1904:26) om vissa internationella rättsförhållanden rörande äktenskap och förmynderskap, som anger att den som är bosatt i en viss stat anses vid tillämpning av lagen ha hemvist där, om bosättningen med hänsyn till vistelsens varaktighet och omständigheterna i övrigt måste anses stadigvarande. Av förarbetena framgår att i denna definition får anses ligga att personen i fråga har för avsikt att stanna kvar i landet.[2] Begreppet förekommer även i andra sammanhang. Exempelvis är ett av villkoren för naturalisation, det vill säga förvärv av svenskt medborgarskap efter ansökan, att den sökande har hemvist här i landet. Migrationsöverdomstolen har i avgörandet MIG 2013:22 uttalat bland annat att i det sammanhanget avser hemvist faktiskt boende i Sverige med avsikt att stanna kvar i landet stadigt men att något krav på folkbokföring eller någon minsta tid för att redan ha vistats i landet inte uppställs; vistelsen ska dock vara legal. Huvudvikten ligger på det subjektiva villkoret att sökanden har för avsikt att stadigt stanna kvar i landet.[3] En vistelse får inte karaktär av hemvist enbart på grund av att den är långvarig utan en helhetsbedömning får göras, där hänsyn

[2] Kungl. Majt:s proposition 1973:158, s. 80 f.
[3] Jfr *Medborgarskap och identitet*, prop. 1997/98:178, s. 9, MIG 2008:17 och MIG 2013:22.

ska tas till bland annat om personen haft stadigvarande yrke eller tjänst, om han eller hon har haft fast bostad, ett egentligt hem eller bott på hotell, pensionat eller hos släkt eller bekanta.[4] Hemvistvillkoret är inte bundet till den grund på vilken utlänningen vistas i Sverige (se Migrationsöverdomstolens dom i mål nr UM 10383-12). Att avsikten hos den enskilde att stadigvarande stanna kvar i landet är av avgörande betydelse för om han eller hon anses ha sin hemvist i Sverige framgår av praxis i ärenden om naturalisation. Det har anförts att hemvistbegreppet innebär att en utlänning, som kommer hit för att bosätta sig, anses ha haft hemvist i landet från den tidpunkt han eller hon ansökte om uppehållstillstånd för bosättning, om han eller hon därefter får sin ansökan bifallen (se exempelvis MIG 2008:17 och MIG 2013:22). Att bedömningen av om hemvist föreligger i viss mån kan knytas till om den enskilde är bosatt i landet framgår av förarbetena till lagen (2008:552) om katastrofmedicin som en del av svenska insatser utomlands; i det sammanhanget anses en person som är bosatt i Sverige i folkbokföringslagens (1991:481) mening ha sitt hemvist i landet.[5]

Sammantaget framträder alltså två huvudsakliga kriterier för hemvist: den enskilde ska anses vara bosatt i Sverige och ha för avsikt att stanna kvar stadigvarande. Med utgångspunkt i dessa kriterier bedömer vi att det normalt finns ett behov av att låta personer som har sin hemvist i Sverige omfattas av ett system för biometrisk verifiering av identitet. Detta bör beaktas vid de överväganden avseende personkretsen som vi gör nedan. Ett undantag som kan noteras redan här är att den som vistas i Sverige som diplomat eller anhörig till diplomat inte anses ha hemvist i Sverige.[6] Vi återkommer i avsnitt 12.4.6 till överväganden avseende sådana personer.

12.2.2 Att vara bosatt i Sverige

Frågan om någon kan anses vara bosatt i Sverige kan ha betydelse bland annat vid folkbokföring, vid bedömningen av rätten till förmåner som regleras i socialförsäkringsbalken och i ärenden om uppehållstillstånd som grundar sig på familjeåterförening. Svensk rätt använder flera olika bosättningsbegrepp vars innebörden varierar

[4] *Hemvist*, SOU 1976:39, s. 128 f.
[5] *Katastrofmedicin som en del av svenska insatser utomlands*, prop. 2007/08:138, s. 42.
[6] Prop. 1975/76:136 om ändringar i lagen (1950:382) om svenskt medborgarskap, s. 55.

inom olika rättsområden och flera författningar har egna definitioner av bosättning för att den specifika författningens syfte ska kunna uppfyllas.[7]

Enligt 3 § folkbokföringslagen anses en person vara bosatt i landet om han eller hon kan antas komma att regelmässigt tillbringa sin dygnsvila här under minst ett år. En person ska anses regelmässigt tillbringa sin dygnsvila här i landet om han eller hon under sin normala livsföring tillbringar dygnsvilan här minst en gång i veckan eller i samma omfattning men med en annan förläggning i tiden. Högsta förvaltningsdomstolen har i HFD 2017 ref. 32 uttalat att det inte är en förutsättning för folkbokföring – vilket i sig kräver att personen anses bosatt här – av en utlänning som måste ha uppehållstillstånd för att få vistas här att tillståndet har en giltighetstid om minst ett år. Uppehållstillståndets längd kan dock, tillsammans med andra omständigheter, ha betydelse för bedömningen av om en person kan antas komma att regelmässigt tillbringa sin dygnsvila i landet under minst ett år.[8]

När det gäller bosättningsbegreppet i 5 kap. 2 § socialförsäkringsbalken utgår det från om den enskilde har sitt egentliga hemvist här i landet. Av förarbetena till bestämmelsen framgår att begreppet bosatt i största möjliga utsträckning ska användas i dess betydelse enligt normalt språkbruk och återspegla de faktiska förhållandena. Den enskildes normala vistelseort bör tillmätas avgörande betydelse. Vid bedömningen av någons egentliga hemvist kan vägledning hämtas i folkbokföringslagen, vilket innebär att även inom socialförsäkringen är den så kallade dygnsviloprincipen avgörande vid bedömningen av var någon har sin egentliga hemvist.[9] I praxis har uttalats att en person som behöver uppehållstillstånd för att få vistas i Sverige kan anses bosatt här i socialförsäkringsbalkens mening även om vederbörande saknar sådant tillstånd (se HFD 2024 ref. 17). I ett annat avgörande ansågs en person som sedan mer än ett år hade suttit frihetsberövad utomlands inte bosatt i Sverige i socialförsäkringsbalkens mening (se HFD 2024 ref. 27).

Uppehållstillstånd kan beviljas på grund av anknytning till personer som är bosatta i Sverige eller har beviljats uppehållstillstånd för bosättning. I förarbetena till 5 kap. 3 a § första stycket 3 utlännings-

[7] *Kvalificering till socialförsäkringen,* prop. 2025/26:136, s. 28.
[8] *Tillfälliga begränsningar av möjligheten att få uppehållstillstånd i Sverige*, prop. 2015/16:174, s. 31.
[9] *Socialförsäkringens personkrets*, prop. 1998/99:119, s. 89 och prop. 2025/26:136, s. 17.

lagen (2005:716) framgår att begreppet bosatt i Sverige ska ges den innebörd som framgår av bestämmelserna i folkbokföringslagen.[10] Med begreppet *uppehållstillstånd för bosättning* avses i regel ett permanent uppehållstillstånd men även personer som beviljats tidsbegränsade uppehållstillstånd som överstiger ett år och har välgrundade utsikter att beviljas permanent uppehållstillstånd kan utgöra anknytningspersoner.[11]

Även om innebörden av olika bosättningsbegrepp kan skilja sig åt i olika sammanhang bedömer vi att personer som enligt någon författning bedöms vara bosatta här generellt kan antas ha en sådan anknytning till landet som talar för att hans eller hennes identitet kan behöva verifieras i olika sammanhang. Denna krets av personer behöver därför som utgångspunkt kunna omfattas av ett system för biometrisk verifiering av identitet.

12.2.3 Annan anknytning till Sverige

Utöver de personer som är bosatta eller har sin hemvist i Sverige kan det finnas de som av olika skäl har en sådan anknytning till landet att det generellt sett finns ett behov av att kunna verifiera deras identitet biometriskt. Som ett resultat av den fria rörligheten inom EU har det blivit allt vanligare att personer vistas såväl kortare som längre perioder i Sverige, även om de inte bedöms vara bosatta eller bedöms ha sin hemvist i landet. I förarbetena till lagen (2022:1697) om samordningsnummer pekades på att det finns personer som av olika anledningar vistas stadigvarande i landet och att de därför får anses ha en förhållandevis stark anknytning till landet även om de inte ska folkbokföras.[12]

Någon entydig definition av vad som avses med att en person har anknytning till Sverige saknas i svensk rätt, även om det förekommer i några olika författningar. Av 1 § lagen om katastrofmedicin som en del av svenska insatser utomlands framgår exempelvis att med människor med anknytning till Sverige avses svenska medborgare, svenska medborgares utländska familjemedlemmar, och i Sverige

[10] *Enklare regler om uppehållstillstånd för vissa vårdnadshavare som sammanbor med barn i Sverige*, prop. 2013/14:217, s. 25 och 42.
[11] Jfr *Ändrade regler i utlänningslagen*, prop. 2020/21:191, s. 82 och MIG 2007:29.
[12] *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, prop. 2020/21:160, s. 47.

bosatta utlänningar. Av 3 § andra stycket rennäringsförordningen (1993:384) framgår att med *närmare anknytning till Sverige* avses att personen i fråga äger en fastighet i Sverige, driver näringsverksamhet i Sverige, har anställning i Sverige eller liknande. En anknytning som bygger endast på svenskt medborgarskap behöver enligt vår bedömning inte nödvändigtvis medföra ett behov för svenska myndigheter att verifiera identitet, om personen inte är bosatt eller kan anses ha hemvist i Sverige. Inte heller i övrigt behöver en anknytning till Sverige i sig ge upphov till ett sådant behov.[13] Att någon är ekonomiskt verksam i landet på sådant sätt som anges i rennäringsförordningen talar däremot för att personen kan förväntas ha kontakt med svenska myndigheter och andra aktörer i sammanhang där identiteten kan behöva verifieras; sådana personer anses ofta vara skatterättsligt bosatta i Sverige även om de inte är bosatta i landet enligt folkbokföringslagen. Exempelvis kan en utländsk person som äger ett fritidshus ofta vara i behov av ett samordningsnummer i kontakt med myndigheter och för att ingå avtal om el eller liknande, vilket också får anses tala för ett behov av att verifiera identiteten i sådana sammanhang.

Att någon har vistats i landet under en längre tid behöver inte i sig visa på en anknytning, utan det är den faktiska etableringen och de band som uppkommit under vistelsen som bör vara av avgörande betydelse. Sådana faktorer beaktas bland annat vid utvisning på grund av brott, enligt 8 a kap. 2 § utlänningslagen.[14] Familjeförhållanden är också av betydelse, särskilt om en utlänning har underåriga barn som är bosatta i Sverige.

Vi anser att det inte är möjligt eller lämpligt att här lämna någon heltäckande uppräkning av vilka personkategorier som kan ha en sådan anknytning till Sverige att det därför också finns ett behov av att låta dem omfattas av ett system för biometrisk verifiering av identitet. Det är inte heller syftet med denna översikt. Vi kan emellertid konstatera att en anknytning till Sverige av sådant slag som vi har gett exempel på ovan ofta kan vara en indikation på att det finns ett behov för myndigheter att kunna verifiera identitet i olika sammanhang.

[13] Jfr behovet av identitetsbeteckning i *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, prop. 2021/21:160, s. 54.
[14] *Ett skärpt regelverk om utvisning på grund av brott*, SOU 2025:54, s. 117.

12.3 Personkategorier som det finns ett behov av att registrera i ett identitetsindex

Med ovanstående utgångspunkter kan vi konstatera att en möjlighet att biometriskt verifiera identitet potentiellt sett kan behöva omfatta en stor krets av personer. I detta avsnitt belyser vi närmare ett flertal personkategorier som kan vara aktuella och som vi anser att det finns ett behov av att låta ingå i ett identitetsindex, för att ett sådant index ska kunna vara till nytta. I nästa kapitel bedömer vi när och för vem en registrering i ett index bör göras, med beaktande bland annat av möjligheterna att ta upp biometriska underlag för vissa kategorier av personer som vi i sig anser behöver omfattas.

12.3.1 Personer som är eller har varit folkbokförda i Sverige

Vår bedömning

Det finns ett behov av att den som är eller har varit folkbokförd i Sverige omfattas av ett identitetsindex.

Enligt 3 § folkbokföringslagen ska den som efter inflyttning anses vara bosatt i Sverige folkbokföras. Med bosatt i Sverige avses i folkbokföringslagens mening att en person kan antas komma att regelmässigt tillbringa sin dygnsvila i landet under minst ett år. Även den som kan antas komma att regelmässigt tillbringa sin dygnsvila både inom och utom landet ska folkbokföras om han eller hon med hänsyn till samtliga omständigheter får anses ha sin egentliga hemvist här. Med hänsyn till de kriterier som gäller för folkbokföring finns det skäl att anta att personer som är folkbokförda i Sverige generellt sett har en sådan anknytning till landet som talar för att hans eller hennes identitet kan behöva verifieras i olika sammanhang. Att vara folkbokförd har i vissa sammanhang bedömts fungera som en nyckel för att kunna delta i samhället.[15] Åtgärder har dock vidtagits för att underlätta för personer som inte är folkbokförda och saknar personnummer.[16]

Uppgifterna i folkbokföringen har stor spridning i samhället och används i stor utsträckning som underlag av myndigheterna i deras

[15] *Personnummer och samordningsnummer*, SOU 2008:60, s. 133.
[16] Se bland annat *Stärkt system för samordningsnummer,* prop. 2021/22:276.

beslutsfattande. Ett antal förmåner är på ett eller annat sätt kopplade till folkbokföringen eller folkbokföringslagens bestämmelser om när en person ska anses som bosatt i landet. Exempelvis följer av bestämmelsen i 8 kap. 1 § hälso- och sjukvårdslagen (2017:30) att regionen ska erbjuda en god hälso- och sjukvård åt den som är bosatt inom regionen. En liknande bestämmelse finns i 5 § tandvårdslagen (1985:125). Med bosättning avses i dessa bestämmelser det samma som i folkbokföringslagen.[17] Med folkbokföring kan även följa en rätt att rösta i kommunala val, även för tredjelandsmedborgare. Den som är folkbokförd kan i nuläget ansöka om ett sådant identitetskort för folkbokförda som utfärdas av Skatteverket[18], och kommer att kunna få ett sådant statligt identitetskort utan resefunktion som Polismyndigheten enligt förslag ska kunna utfärda.[19]

Det personnummer som den enskilde får i samband med folkbokföringen utgör en identitetsbeteckning och används i stor utsträckning i samhället. Personnumret fungerar bland annat som ett hjälpmedel för att kunna identifiera en person och som ett sökbegrepp i it-system som gör det enklare att utbyta information mellan myndigheter. Det är också en förutsättning för att kunna skaffa ett BankID. Personnumret kan anses i sig innebära en viss säkerhet, exempelvis i en avtalssituation för den enskildes avtalspart, för att ett avtal kommer att fullföljas av den enskilde. Den som är folkbokförd i Sverige och därmed har ett personnummer anses ha en mycket stark anknytning till Sverige.[20]

Av det ovan anförda framgår enligt vår mening att det finns ett tydligt behov att kunna verifiera identiteten för den som är folkbokförd i Sverige. Den som är folkbokförd i Sverige kan av olika anledningar avregistreras, vanligtvis på grund av att han eller hon flyttar från landet under en viss tid; av 20 § folkbokföringslagen framgår att som huvudregel ska den som kan antas komma att regelmässigt tillbringa sin dygnsvila utom landet under minst ett år avregistreras från folkbokföringen som utflyttad. Vi anser att det finns ett behov av att även personer som har varit folkbokförda ska kunna omfattas av ett identitetsindex. Detta med hänsyn dels till att personen behåller sitt personnummer även om en avregistrering sker,

[17] Jfr *En ny hälso- och sjukvårdslag*, prop. 2016/17:43, s. 137 och *Skydd för förföljda personer, samordningsnummer, m.m.*, prop. 1997/98:9, s. 49.
[18] Se dock *Avveckling av Skatteverkets id-kortsverksamhet,* Fi2026/01416, juni 2026.
[19] Promemorian *Ett statligt identitetskort,* Ju2026/01595, s. 183 f.
[20] Prop. 2021/22:276, s. 41.

dels till att det inte är osannolikt att personen återkommer till Sverige eller på annat sätt behåller en anknytning till landet trots avregistreringen, exempelvis genom ett svenskt medborgarskap. En avregistrering kan enligt 21 § folkbokföringslagen även avse personer som inte anses bosatta på någon fastighet eller i någon kommun. Det kan emellertid antas att dessa personer vistas i landet, varför det kan finnas ett behov av att biometriskt verifiera deras identitet i olika sammanhang.

12.3.2 Personer som har tilldelats ett samordningsnummer

Vår bedömning

Det finns ett behov av att den som har tilldelats ett samordningsnummer omfattas av ett identitetsindex. Detta gäller oavsett om numret har tilldelats efter ansökan från den enskilde eller begäran av en annan aktör.

Det huvudsakliga syftet med samordningsnummer är att tillgodose myndigheternas behov av ett enhetligt nummer för att undvika personförväxling och för att kunna utbyta information med andra myndigheter och organisationer om individer som vistas tillfälligt här i landet eller som har rätt till olika förmåner utan att vistas här.[21] Det finns därför en möjlighet att tilldela någon ett samordningsnummer efter begäran av en myndighet eller ett sådant annat organ som regeringen bestämmer, enligt 2 kap. 1 § 1 lagen om samordningsnummer. Samordningsnumren har fått en stor betydelse i samhället. De används bland annat vid kontakter med myndigheter, men även vid kontakter med andra, exempelvis sjukvården, banker och privata företag. Redan dessa omständigheter talar enligt vår bedömning tydligt för att det finns ett behov av att låta den som har ett samordningsnummer omfattas av ett identitetsindex.

Som vi pekat på i avsnitt 12.2.3 kan samordningsnummer ofta behöva tilldelas personer som av olika anledningar vistas stadigvarande i landet och som därför kan ha en anknytning till landet, även om de inte ska folkbokföras. Ett samordningsnummer kan därför även tilldelas efter egen ansökan, om den enskilde har en

[21] *Personnummer och samordningsnummer*, prop. 2008/09:111, s. 30.

sådan anknytning till Sverige att han eller hon kan antas behöva en identitetsbeteckning. Det kan enligt förarbetena till 2 kap. 1 § lagen om samordningsnummer till exempel vara att den enskilde eller någon annan i familjen äger fast egendom, en tomträtt eller en bostadsrätt eller innehar en hyresrätt. För de som efter egen ansökan tilldelas ett samordningsnummer kan det därför, enligt vår mening, antas finnas ett behov av att verifiera identiteten i många sammanhang. Det kan också vara fråga om exempelvis EES-medborgare som med stöd av den fria rörligheten vistas i Sverige för tillfälliga arbeten, forskning eller kortare studier.[22] Enligt förslag i betänkandet *Registrering av EES-medborgare* ska en registreringsskyldighet återinföras för vissa EES-medborgare som vistas i Sverige i mer än tre månader. Migrationsverket föreslås utfärda ett registreringsbevis till registrerade EES-medborgare och i samband med det begära ett samordningsnummer hos Skatteverket, om EES-medborgaren inte är eller har varit folkbokförd eller redan har tilldelats ett samordningsnummer.[23] Det rör sig sammantaget om personer som vanligtvis har någon form av ekonomiska intressen i Sverige.

Samordningsnummer kan användas i brottsliga syften. Förutom felaktiga utbetalningar från välfärdssystemen har missbruk av samordningsnummer upptäckts i form av att en person använder en annan persons samordningsnummer, exempelvis som fordonsmålvakt. Samordningsnumret kan användas för att registrera ett stort antal fordon. Det kan bland annat leda till svårigheter med att driva in fordonsrelaterade skatter och avgifter. Det förekommer också att målvaktsfordon används som brottsverktyg i olika kriminella sammanhang.[24] För att motverka sådant utnyttjande av identiteter kan verifiering, i synnerhet med hjälp av biometriska uppgifter, mot ett identitetsindex vara av stort värde. Detta talar, enligt vår bedömning, också starkt för ett behov av att låta personer som har tilldelats ett samordningsnummer omfattas av personkretsen.

[22] Prop. 2020/21:160, s. 53 ff. och prop. 2021/22:276, s. 47.
[23] SOU 2026:9, s. 119 och 170.
[24] Prop. 2021/22:276, s. 30.

12.3.3 Personer med uppehållstillstånd

Vår bedömning

Det finns ett behov av att den som har ett uppehållstillstånd med en giltighetstid som överstiger ett år omfattas av ett identitetsindex.

För andra utlänningar än EES-medborgare med uppehållsrätt är ett giltigt uppehållstillstånd, som utgångspunkt, en grundförutsättning för att få vistas i Sverige. Uppehållstillstånd kan, enligt 2 kap. 4 § utlänningslagen, vara tidsbegränsade eller permanenta. Uppehållstillstånd kan beviljas på många olika grunder. Vissa tillstånd beviljas uttryckligen med hänsyn till att personen har en anknytning till Sverige, antingen genom en anhörig eller av andra skäl. Sådana uppehållstillstånd beviljas generellt med en giltighetstid om två år, enligt 5 kap. 3 g § andra stycket utlänningslagen. Personer som beviljas ett tillstånd på dessa grunder kan generellt antas komma att vistas i landet under sådan tid att de kommer att vara bosatta i landet, och även kommer att ha sin hemvist här. Under vistelsen kan de därmed antas komma i kontakt med myndigheter och andra aktörer i förhållandevis stor utsträckning, vilket talar starkt för att deras identitet kan behöva verifieras i olika sammanhang. Detsamma gäller enligt vår mening för personer som beviljas uppehållstillstånd på grund av skyddsbehov eller synnerligen ömmande omständigheter. I sistnämnda fall kan uppehållstillstånd bland annat beviljas med hänsyn till att det föreligger ett bestående verkställighetshinder (se MIG 2008:38 och MIG 2019:4); det kan då med fog antas att personen kommer att vistas i Sverige under en längre tid.

Sammantaget anser vi att det finns ett behov av att, som utgångspunkt, låta den som beviljats ett permanent eller tidsbegränsat uppehållstillstånd omfattas av ett identitetsindex. Vissa undantag är emellertid påkallade, vilket vi redogör för nedan.

Uppehållstillstånd som gäller i högst ett år

Enligt 5 kap. 10 § utlänningslagen kan uppehållstillstånd beviljas för bland annat besök. Avgörande för att ett tidsbegränsat uppehållstillstånd för besök kan beviljas är att det står klart att det är fråga

om en besöksvistelse och att den sökande alltså inte kan antas komma att arbeta illegalt eller avser att bosätta sig här. Ett uppehållstillstånd för besök beviljas i regel inte för längre tid än totalt ett år, eftersom sökanden då skulle ha rätt att folkbokföra sig i Sverige och vistelsen inte längre skulle ha karaktären av ett besök (se MIG 2008:15). När det gäller personer som vistas i Sverige med ett uppehållstillstånd för besök anser vi att de inte kan anses ha en sådan anknytning till landet att det finns ett behov av att registrera dem i ett identitetsindex.

I 5 kap. utlänningslagen finns även andra bestämmelser som reglerar tidsbegränsade uppehållstillstånd. Bland annat får ett tillstånd beviljas en utlänning som önskar vistas här i landet för att söka arbete eller undersöka förutsättningarna för att starta näringsverksamhet, i enlighet med 9 §. Enligt 12 § får ett tidsbegränsat tillstånd beviljas en utlänning som vårdas med stöd av lagen (1990:52) med särskilda bestämmelser om vård av unga. Ett tidsbegränsat tillstånd om minst sex månader ska även under vissa förutsättningar beviljas enligt 15 § om det behövs för att förundersökning eller huvudförhandling i brottmål ska kunna genomföras.

Den som beviljas ett uppehållstillstånd med en giltighetstid som inte överstiger ett år kan normalt sett inte antas vistas i landet under en sådan tid att han eller hon ska anses bosatt i landet, och ska därför inte heller folkbokföras. I praxis har samtidigt uttalats att det inte är en nödvändig förutsättning för folkbokföring av en utlänning som måste ha uppehållstillstånd för att få vistas här, att tillståndet har en giltighetstid om minst ett år (se HFD 2017 ref. 32). Utgångspunkten bör enligt vår mening vara att den som beviljats ett uppehållstillstånd som inte överstiger ett år inte enbart genom beviljandet av tillståndet kan antas få en sådan anknytning till Sverige att hans eller hennes identitet kan behöva verifieras biometriskt mot ett identitetsindex. De grunder som nämnda, kortare uppehållstillstånd, kan beviljas på är generellt sådana att det inte kan förväntas att personen kommer att stanna kvar i landet stadigvarande. Om så ändå är fallet ska personen folkbokföras. Vid tidpunkten för folkbokföring bör personen däremot omfattas av den personkrets för vilken det finns ett behov av att omfattas av ett identitetsindex. Mot denna bakgrund anser vi att det saknas behov av att låta personer som har beviljats uppehållstillstånd med en giltighetstid som inte överstiger ett år omfattas av ett index.

Personer som beviljats uppehållstillstånd innan inresa

Syftet med ett sådant identitetsindex som vi anser bör övervägas är i första hand att det ska kunna användas för att verifiera identitet på personer som vistas i landet, i andra ärendeslag och sammanhang än de ärenden där en grundidentitet kan behöva etableras som handläggs av Polismyndigheten, Migrationsverket och Skatteverket. Det kan därför ifrågasättas om det finns behov av att registrera en person som har beviljats ett uppehållstillstånd – oavsett längden på tillståndet – men inte befinner sig i Sverige. Till detta kommer att när personen faktiskt reser in till Sverige och anmäler inflyttning finns en möjlighet att verifiera identiteten i ärendet om folkbokföring. Det är vidare först i samband med inresan – dock under förutsättning att uppehållstillståndet inte endast medger en kortare vistelse än ett år – som en sådan anknytning till landet kan sägas uppstå som innebär att personen omfattas av den personkrets som vi anser bör registreras i ett identitetsindex.

Mot det ovan anförda kan ställas att även om en utlänning, enligt 26 § folkbokföringslagen, *ska* anmäla inflyttning kan det förekomma att en person av olika skäl inte gör detta och ändå vistas i Sverige. Enligt vår mening är det viktigt att en registrering i ett identitetsindex inte underlåts av det skälet. Vi kan också konstatera att möjligheten att ta upp biometriska underlag enligt 26 b § folkbokföringslagen är i viss mån begränsad, vilket vi återkommer till i avsnitt 13.3.6. Som vi ser det är det också en fördel om en person som – genom att ha ansökt om och beviljats ett uppehållstillstånd som kan ligga till grund för folkbokföring i Sverige – har visat att han eller hon har en avsikt att vistas i landet kan omfattas i ett tidigt skede. Detta kan underlätta verifiering av personens identitet vid inresa och vid anmälan om inflyttning. Utgångspunkten måste, som vi ser det, vara att en person som innan inresa har beviljats ett längre uppehållstillstånd också har för avsikt att resa in och vistas i Sverige. Att det i undantagsfall kan vara så att en person registreras i ett identitetsindex utan att han eller hon därefter faktiskt vistas i Sverige är därför inte – även med hänsyn till principen om uppgiftsminimering – ett skäl som talar mot att denna krets av personer bör kunna omfattas.

12.3.4 Personer med ställning som varaktigt bosatta

Vår bedömning

Det finns ett behov av att en utlänning som har ställning som varaktigt bosatt i Sverige omfattas av ett identitetsindex.

Av 5 a kap. 1 § utlänningslagen framgår att en ansökan från en utlänning om ställning som varaktigt bosatt i Sverige ska beviljas om sökanden de senaste fem åren utan avbrott har vistats i Sverige med uppehållstillstånd eller på någon annan grund som lagligen bosatt. Bestämmelsen tar alltså sikte på personer som vistats under längre tid i landet. Ställning som varaktigt bosatt ska enligt 4 § 2 inte beviljas en utlänning vars vistelse i Sverige inte är av varaktig karaktär. Det kan exempelvis handla om personer som har ett lagakraftvunnet beslut om av- eller utvisning, men som har fått ett tillfälligt uppehållstillstånd på grund av verkställighetshinder.[25] Bosättningstiden bör vara ett av de viktigare kriterierna och för att omfattas av direktivet om varaktigt bosatta[26] bör bosättningen ha varit laglig och oavbruten för att vittna om personens förankring i landet (se skäl 6 till direktivet). Med lagligen bosatt avses att utlänningen, utöver att ha vistats i Sverige med uppehållstillstånd, har vistats i landet med uppehållsrätt eller permanent uppehållsrätt eller under vistelsen har varit undantagen från kravet på att inneha ett uppehållstillstånd (se MIG 2024:4).

Den personkrets som kan beviljas ställning som varaktigt bosatt i Sverige utgörs alltså av personer som varit bosatta i landet under längre tid och som har en stark anknytning hit. Det får vidare antas att de är folkbokförda i landet, vilket innebär att de kan omfattas av personkretsen för ett identitetsindex redan av den anledningen. Det kan dock finnas situationer när så inte är fallet. Mot denna bakgrund anser vi att det finns behov av att en utländsk medborgare som har ställning som varaktigt bosatt i Sverige omfattas av ett index.

[25] *Uppföljning av återvändandedirektivet och direktivet om varaktigt bosatta tredjelandsmedborgares ställning*, prop. 2016/17:61, s. 35.
[26] Rådets direktiv 2003/109/EG av den 25 november 2003.

12.3.5 Svenska medborgare

Vår bedömning

Det finns ett behov av att svenska medborgare omfattas av ett identitetsindex.

Ett identitetsindex kommer i praktiken – enligt vår bedömning – till allra största del att ta sikte på att verifiera identitet för svenska medborgare. Den som är svensk medborgare har normalt sett en naturlig och stark anknytning till landet genom att han eller hon är bosatt och har sin hemvist här. Därigenom har personen som utgångspunkt också ofta kontakt med svenska myndigheter och andra aktörer i samhället, vilket talar starkt för ett behov av att kunna verifiera identitet mot ett identitetsindex.

Att svenska medborgare bör ingå i den personkrets som omfattas av ett identitetsindex framstår med hänsyn till det ovan anförda som givet. Medborgarskapet som sådant medför enligt vår mening närmast en presumtion för att det finns en sådan anknytning till Sverige att personen också bör omfattas av personkretsen. Med medborgarskapet följer flera särskilda rättigheter, däribland en absolut rätt att bo och arbeta i Sverige och en rätt att rösta i riksdagsval. Som vi nämnt i avsnitt 12.2.3 anses svenska medborgare, oavsett om de är bosatta eller har hemvist i Sverige, ha en sådan anknytning till landet att de omfattas av lagen om katastrofmedicin som en del av svenska insatser utomlands.

Även med hänsyn till det ovan anförda kan vi konstatera att behovet av att verifiera identitet mot ett nationellt identitetsindex kan antas vara mindre för svenska medborgare som mer varaktigt är bosatta utomlands. Det kan enligt vår mening därför övervägas om svenska medborgare som är avregistrerade från folkbokföringen som utflyttade inte bör omfattas av ett index. Av 20 § folkbokföringslagen framgår att bland annat personer som kan antas komma att regelmässigt tillbringa sin dygnsvila utom landet under minst ett år ska avregistreras från folkbokföringen som utflyttad. Det är alltså fråga om en längre tidsperiod under vilken personen inte kommer att vistas i Sverige. Folkbokföring är, som vi pekat på i avsnitt 12.3.1, som utgångspunkt en nyckel för att kunna delta i samhället och ligger vanligen till grund för rätten till bosättningsbaserade socialförsäk-

ringsförmåner. För den som är avregistrerad från folkbokföringen som utflyttad kan behovet av att verifiera identitet därmed som utgångspunkt antas vara begränsat. Personer som flyttar utomlands och avregistreras från folkbokföringen, men som fortfarande har rätt till svensk pension, behöver dock upprätthålla kontakt med svenska myndigheter årligen för att visa att de fortfarande lever och det förekommer att personer hämtar ut anhörigas pension även efter att de avlidit i utlandet. Av praxis framgår att det även i fall där personen varit utflyttad men har arbetat på distans för en arbetsgivare i Sverige har funnits en rätt till arbetsbaserade förmåner enligt socialförsäkringsbalken (se HFD 2022 ref. 16). Behov av att verifiera identitet kan antas finnas i dessa situationer. Den som är bosatt utomlands kan också ha kvar en skattemässig anknytning till landet, exempelvis genom att personen har innehav av andelar i handelsbolag som äger betydande affärs- och hyresfastigheter i Sverige (se RÅ 1989 ref. 103), som innebär att de har viss kontakt med svenska myndigheter. Svenska medborgare som bor utomlands kan också äga exempelvis fritidsfastigheter eller annan egendom som innebär att ett samordningsnummer hade kunnat behöva tilldelas, om personen saknat en identitetsbeteckning.

Om endast svenska medborgare med en viss form av anknytning till Sverige bör omfattas av personkretsen krävs bedömningar i det enskilda fallet som inte når upp till kravet på förutsebarhet. Personer som är avregistrerade som utvandrade kan i många fall antas ha en mer begränsad kontakt med svenska myndigheter, vilket innebär att deras identitet inte nödvändigtvis kan behöva verifieras mot ett identitetsindex. Även med hänsyn till detta anser vi att medborgarskapet i sig medför en sådan bestående anknytning till landet att enbart den omständigheten att en person är avregistrerad som utvandrad i folkbokföringen inte medför att det saknas behov av att registrera honom eller henne i ett identitetsindex. En registrering i ett identitetsindex förutsätter emellertid att biometriska underlag kan tas upp i samband med registreringen. En viss avgränsning av vilka svenska medborgare som de facto kommer att registreras kan därför komma att göras på det sättet, men förändrar inte vår bedömning att det finns ett behov av generellt sett att låta svenska medborgare omfattas av ett index. Vi återkommer till detta i kapitel 13.

12.3.6 Personer med kvalificerade skyddsidentiteter

Vår bedömning

Det finns ett behov av att kvalificerade skyddsidentiteter omfattas av ett identitetsindex.

En kvalificerad skyddsidentitet är en särskilt beslutad identitet som består av andra personuppgifter än de verkliga och som har förts in i statliga register eller i handlingar som utfärdats av statliga myndigheter. Kvalificerade skyddsidentiteter får användas av anställda vid Polismyndigheten, Säkerhetspolisen och Försvarsmakten, under vissa förutsättningar. Eftersom ett identitetsindex av det slag vi anser bör övervägas endast ska innehålla unika identiteter, vilket säkerställs genom en unik alfanumerisk nyckel till vilken biometriska uppgifter kopplas, uppkommer frågan om det bör vara möjligt att registrera en individ dels med hans eller hennes riktiga identitet, dels med en kvalificerad skyddsidentitet; de biometriska uppgifterna skulle då förekomma under två olika identiteter.

En person med kvalificerad skyddsidentitet kan ha behov av att agera i samhället med användande av skyddsidentiteten och av att verifiera denna identitet i olika sammanhang. Av förarbetena till lagen (2006:939) om kvalificerade skyddsidentiteter framgår att i motsats till vad som gäller vid tillämpningen av lagen om fingerade personuppgifter bör tjänstemannens verkliga personuppgifter inte avregistreras från folkbokföringen när de fiktiva personuppgifterna förs in. Skälet till det är att tjänstemän med skyddsidentitet måste kunna upprätthålla privatliv och tjänstgöring parallellt. Normalt måste de dessutom parallellt kunna fullgöra vissa tjänsteåligganden med användande av sina verkliga personuppgifter och andra tjänsteåligganden med användande av skyddsidentitetens fiktiva personuppgifter. En avregistrering av de verkliga personuppgifterna skulle för övrigt göra ett system för skyddsidentiteter mer sårbart för kartläggning och avslöjanden.[27] Sistnämnda problematik skulle kunna göra sig gällande om en identifiering med biometriska uppgifter mot ett identitetsindex skulle ge två träffar, en för den verkliga identiteten och en för den kvalificerade skyddsidentiteten.

[27] *Kvalificerad skyddsidentitet*, prop. 2005/06:149, s. 45.

Med hänsyn till en tjänstemans behov av att kunna använda en kvalificerad skyddsidentitet på samma sätt som den verkliga identiteten anser vi att det som utgångspunkt finns ett behov av att låta även kvalificerade skyddsidentiteter ingå i ett index, eftersom syftet med ett sådant system i första hand är att verifiera identitet vid kontakt med myndigheter. Om det inte skulle vara möjligt för en tjänsteman att använda en kvalificerad skyddsidentitet i sådana sammanhang motverkas syftet med skyddsidentiteten.

Vid en verifiering behöver först en lokalisering av en viss individ som är registrerad i ett index ske med hjälp av en alfanumerisk nyckel eller andra alfanumeriska uppgifter – exempelvis personnummer – och en jämförelse sedan göras med hjälp av de biometriska uppgifter som är kopplade till träffen. Det skulle därför inte uppstå några problem i praktiken vid verifiering av identitet, utan det kan göras på samma sätt som om tjänstemannen använder sin riktiga identitet. Den aktör som verifierar identiteten skulle inte se annat än den identitet som kontrolleras vid ett givet tillfälle. Det skulle därför inte heller vid en verifiering uppstå risk för att den kvalificerade skyddsidentiteten röjs, genom den koppling mellan den riktiga identiteten och den fingerade som finns, i form av att samma biometriska uppgifter är registrerade för båda. En sådan sammankoppling kan däremot uppkomma om en identifiering görs, det vill säga att en en-till-många-jämförelse genomförs mot ett identitetsindex, med biometriska uppgifter. En identifiering bör, som vi återkommer till i avsnitt 13.2.1 och 18.2.1, endast göras i samband med att en person registreras i ett identitetsindex. På det sättet säkerställs att multipla identiteter inte kan skapas i indexet. En identifiering, i samband med registrering av en kvalificerad skyddsidentitet, skulle ge en träff på den verkliga identiteten, om denna redan är registrerad. Detta skulle röja den kvalificerade skyddsidentiteten, vilket naturligtvis inte får ske.

En möjlig lösning skulle kunna vara att en registrering sker i identitetsindexet i samband med att ett beslut om kvalificerad skyddsidentitet fattas, av relevant myndighet, utan att en identifiering görs. Av 4 § lagen om kvalificerade skyddsidentiteter framgår att det i ett sådant beslut får förordnas om bland annat att Transportstyrelsen ska utfärda körkort i den kvalificerade skyddsidentitetens namn och att andra statliga myndigheter ska utfärda pass eller andra identitetshandlingar i den kvalificerade skyddsidentitetens namn. En möjlighet

att även förordna att den kvalificerade skyddsidentiteten registreras i ett identitetsindex skulle medföra att den – och den verkliga identiteten – skulle kunna existera parallellt i systemet.

Våra närmare överväganden i dessa avseenden finns i avsnitt 13.3.8. I detta sammanhang stannar vi vid bedömningen att det finns ett behov av att låta även kvalificerade skyddsidentiteter omfattas av ett identitetsindex.

12.4 Personkategorier som det saknas ett behov av att registrera i ett identitetsindex

Vi har i föregående avsnitt redogjort för vilka personkategorier som vi anser att det finns ett behov av att inkludera i ett identitetsindex. Vissa avgränsningar har gjorts inom respektive kategori. I detta avsnitt belyser vi de kategorier för vilka vi generellt sett anser att det saknas ett sådant behov.

12.4.1 Barn som inte har fyllt sex år

Vår bedömning

Det saknas behov av att barn som inte har fyllt sex år omfattas av ett identitetsindex.

En särskild fråga är om det finns behov av att registrera barn, det vill säga personer som inte har fyllt 18 år. Eftersom ett identitetsindex behöver bygga på biometriska uppgifter kommer biometriska underlag att behöva tas upp. Barnets bästa är det som i första hand ska beaktas vid alla åtgärder som rör barn och barn ska skyddas från godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv (artikel 3 och 16 i FN:s konvention om barnets rättigheter, barnkonventionen).

I de ärendeslag där en grundidentitet kan behöva bestämmas kan biometriska underlag i de flesta fall tas upp av barn som har fyllt sex år. Behovet för Polismyndigheten och Migrationsverket av att kunna identifiera ett barn eller verifiera ett barns identitet kan visserligen antas vara stort i exempelvis ett ärende om uppehållstillstånd, där

barnet kanske tidigare är okänt för svenska myndigheter; i slutbetänkande av Utredningen om stärkt återvändandeverksamhet lyftes bland annat fram att vissa barn i migrationsprocessen är särskilt sårbara för att bli utsatta för människohandel och exploatering, till exempel ensamkommande barn eller barn som har följt med en förälder som själv utsatts för människohandel eller exploatering.[28] Några vägande skäl för att undanta barn i sådana situationer från ett identitetsindex har enligt vår bedömning inte kommit fram.

Även för andra barn kan det finnas ett behov av att verifiera identitet i olika sammanhang. Ett barns rättshandlingsförmåga får då betydelse. Av 9 kap. 1 § föräldrabalken framgår att den som är under 18 år är omyndig (underårig) och enligt huvudregeln inte får råda över sin egendom eller åta sig förbindelser. En underårig saknar alltså full rättshandlingsförmåga. Det kan därför antas finnas ett begränsat behov för myndigheter och andra aktörer att verifiera identitet för ett barn mot ett identitetsindex, utöver vad som är möjligt genom en kontroll mot en fysisk identitetshandling eller genom uppgifter som lämnas av vårdnadshavarna, när barnet inte har uppnått en sådan mognad att det agerar mer självständigt i olika sammanhang. I många situationer har barn som uppnått viss ålder och mognad dock rätt att agera på egen hand. Exempelvis har en underårig, enligt 9 kap. 3 § första stycket föräldrabalken, rätt att själv råda över egendom som han själv förvärvat genom eget arbete efter fyllda 16 år. Detsamma gäller avkastningen av sådan egendom och vad som trätt i egendomens ställe. Ett barn har därför även rätt att själv föra sin talan i en process rörande sådan egendom. Barn som har fyllt 16 år kan också själv anmäla flytt till, från eller inom Sverige enligt 30 § folkbokföringslagen. I vissa mål enligt lagen med särskilda bestämmelser om vård av unga har den som fyllt 15 år rätt att själv föra sin talan. Ett barn har också, efterhand som det blir äldre, större inflytande i vårdsammanhang, och kan då uppträda även utan vårdnadshavare; barnets inställning ska tillmätas betydelse i förhållande till hans eller hennes ålder och mognad, enligt 4 kap. 3 § patientlagen (2014:821). Att det kan finnas behov av att kunna verifiera identitet i sådana sammanhang har vi belyst i avsnitt 10.7.5.

Det kan alltså finnas behov av att verifiera identiteten för barn i olika sammanhang, även om det naturligtvis inte sker i samma utsträckning som för vuxna.

[28] *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll*, SOU 2024:80, s. 491.

I detta sammanhang bör även lyftas fram att ett identitetsindex inte endast har till syfte att möjliggöra en utökad kontroll av identitet för myndigheter och andra aktörer utan att ett index också ska motverka att enskilda får sina identiteter utnyttjade utan deras vetskap, vilket är ett allt större problem. Barn kan vara särskilt utsatta i sådana sammanhang.

Även med hänsyn till att barns identitet i många fall kan verifieras på ett tillförlitligt sätt mot exempelvis uppgifter i en fysisk identitetshandling eller genom uppgifter som lämnas av vårdnadshavarna, anser vi sammantaget att barn generellt inte bör undantas från den krets av personer som det finns behov av att registrera i ett identitetsindex. En viss lägre åldersgräns bör enligt vår mening dock gälla. Barn som inte har fyllt sex år är undantagna från skyldigheten att lämna fingeravtryck i många av de ärenden där sådana kan tas upp, exempelvis vid en ansökan om uppehållstillstånd (se bland annat 9 kap. 8 a § utlänningslagen). Barn som inte har fyllt sex år har inte heller uppnått en sådan mognad eller ålder att de kan antas ha en egen rättshandlingsförmåga som medför att deras identitet behöver verifieras i samhället annat än i undantagsfall. Med hänsyn till detta anser vi att det saknas behov av att barn som inte har fyllt sex år omfattas av ett identitetsindex. Den tidigare åldersgräns om 14 år som gällde för upptagande av fingeravtryck enligt 9 kap. 8 § utlänningslagen bör enligt vår mening inte övervägas. Detta med hänsyn till att den hade sin grund i tidigare gällande åldersgräns i bland annat Eurodacförordningen[29], som numera har sänkts till sex år.

12.4.2 Personer som ansöker om internationellt skydd

Vår bedömning

Personer som ansöker om internationellt skydd bör inte omfattas av ett identitetsindex.

Den som ansöker om internationellt skydd i Sverige kan normalt antas ha för avsikt att stadigvarande stanna kvar i landet. Som vi pekat på i avsnitt 12.2.1 är avsikten hos den enskilde att stadigvarande stanna kvar i landet av avgörande betydelse för om han eller hon ska anses

[29] Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013.

ha sin hemvist i Sverige. I ärenden om medborgarskap genom naturalisation har detta i praxis inneburit att hemvisttid kan räknas från tidpunkten för en asylansökan, om ansökan bifallits (se MIG 2008:17). Vi kan konstatera att statistik från Migrationsverket visar på att en asylsökande ofta vistas i landet under förhållandevis lång tid, oavsett utgången i ett enskilt ärende. Handläggningstiderna för förstagångsärenden om asyl var i genomsnitt 167 respektive 198 dagar år 2022 och 2023 och den totala genomsnittliga vistelsetiden i mottagningssystemet för utskrivna personer låg under dessa år på sammanlagt 740 respektive 620 dagar.[30] Att många personer kan antas få en anknytning till Sverige under denna tid – inte minst de som har rätt att arbeta under tiden då ansökan prövas – framstår därför som sannolikt. Frågan är därför om det finns behov av att låta personer som ansöker om internationellt skydd omfattas av ett identitetsindex under tiden ansökan behandlas.

I förarbetena till lagen om samordningsnummer diskuterades om asylsökande borde tilldelas en sådan identitetsbeteckning. Som argument för detta anfördes att asylsökande regelmässigt kommer i kontakt med andra myndigheter och aktörer under tiden som de väntar på beslut. Vi delar denna bedömning. Samtidigt lyftes risker fram med att tilldela asylsökande ett samordningsnummer. Bland annat pekades på att de allra flesta nummer skulle registreras med uppgift ”osäker identitet” eftersom det inte sällan saknas identitetshandlingar i det inledande skedet av asylprocessen, och att någon definitiv bedömning av identiteten inte går att göra förrän i samband med ett eventuellt beslut om uppehållstillstånd. Det är också vanligt att det kommer fram nya uppgifter om en sökandes födelsetid under processen om uppehållstillstånd på grund av behov av internationellt skydd, vilket kan komma att skapa problem med spårbarheten om ett nytt nummer ska tilldelas vid dessa tillfällen. Olika nummer som avser samma person skulle då också kunna finnas registrerade hos olika myndigheter och organisationer, vilket kan leda till problem med att följa individen. Det ansågs därmed finnas risk för att samma individ innehar flera olika identitetsbeteckningar under olika identiteter. Det lyftes vidare fram att det saknas möjligheter att lagra biometriska uppgifter och koppla dem till samordningsnumret för framtida jämförelser. Bedömningen gjordes därför att samordningsnummer inte skulle tilldelas asylsökande, utan att det är av större betydelse att

[30] *Budgetpropositionen för 2025*, prop. 2024/25:1, Utgiftsområde 8, s. 9, 11 och 14.

den som beviljas ett uppehållstillstånd snarast får ett personnummer fastställt och använder det som identitetsbeteckning när han eller hon integreras i samhället.[31]

Frånvaro av identitetshandlingar är visserligen vanligt förekommande i ärenden om uppehållstillstånd på grund av behov av internationellt skydd. Polismyndigheten och Migrationsverket har emellertid fått vissa rättsliga verktyg som möjliggör att i större utsträckning söka efter och omhänderta identitetshandlingar (se avsnitt 7.4.2). Screeningförordningen[32] innehåller dessutom bestämmelser som syftar till att förmå personer som ansöker om internationellt skydd att medverka till att överlämna identitetshandlingar och lämna korrekta uppgifter om sin identitet – i annat fall kan ett påskyndat förfarande och ett särskilt gränsförfarande tillämpas. Detta bör i viss utsträckning kunna motverka de problem med att identitet inte kan fastställas förrän sent i processen som pekades på i nämnda förarbeten. Den modell för ett identitetsindex som vi utvärderar, där en unik alfanumerisk nyckel används tillsammans med biometriska uppgifter, bör enligt vår mening också kunna motverka de problem med följbarhet som lyftes fram; även om nya identitetsuppgifter skulle komma fram under handläggningen av ärendet kan dessa knytas till en unik individ i ett sådant index.

En omständighet som däremot talar mot ett behov av att registrera personer som ansöker om internationellt skydd i ett index redan i samband med ansökan är att det är fråga om en relativt liten grupp. Antalet förstagångsansökningar har dessutom minskat de senaste tre åren. Vidare är bifallsfrekvensen förhållandevis låg. Detta framgår av följande tabell.[33]

Tabell 12.1 Inkomna förstagångsansökningar och avgjorda ärenden om asyl

År	2021	2022	2023	2024	2025
Inkomna	11 419	16 738	12 498	9 645	6 735
Avgjorda	12 804	14 245	15 905	11 456	8 339
Bifallsfrekvens	26 %	26 %	26 %	30 %	32 %

[31] Prop. 2021/22:276, s. 111 ff.
[32] Europaparlamentets och rådets förordning (EU) 2024/1356 av den 14 maj 2024.
[33] Uppgifterna har hämtats från Migrationsverkets statistik, https://www.migrationsverket.se/om-migrationsverket/statistik/asyl.html, senast besökt den 2 juli 2026.

Utgångspunkten är att personer som har ett gällande avlägsnandebeslut ska återvända och alltså inte fortsätta att vistas i landet. Det bör därför inte finnas något tydligt behov av att verifiera identitet för personen i detta skede. Vi kan i detta sammanhang även notera att möjligheten till så kallat spårbyte – det vill säga möjligheten att beviljas uppehållstillstånd för arbete efter ett lagakraftvunnet beslut om att avslå en ansökan om internationellt skydd – sedan den 1 april 2025 har utmönstrats. För en majoritet av de som ansöker om sådant skydd skulle därför ett behov av att verifiera identitet föreligga endast under den tid de är sökande; med utgångspunkt i ovanstående statistik skulle det röra sig om cirka 4 000 personer per år. Den som får ett beslut om bifall på ansökan kommer vidare – på det sätt som anfördes i ovan nämnda förarbeten avseende samordningsnummer – att kunna folkbokföras snabbt. Registrering i ett identitetsindex för en person som får bifall på sin ansökan om internationellt skydd bör kunna ske när ett uppehållstillståndskort utfärdas eller när personen folkbokförs i Sverige (se avsnitt 13.3.5 och 13.3.6). Ett reellt behov för myndigheter och andra aktörer av att biometriskt verifiera identitet för en person som ansöker om internationellt skydd kan som vi ser det antas uppkomma först när personen folkbokförs; som vi anfört i avsnitt 12.3.1 fungerar en registrering i folkbokföringen i praktiken, som utgångspunkt, som en nyckel för att kunna delta i samhället och kan ge ligga till grund för olika sociala förmåner.

Vi anser att det ovan anförda talar mot ett behov av att registrera personer som ansöker om internationellt skydd i ett identitetsindex. Behovet av att kunna följa dessa individer och motverka att de uppträder med olika identiteter i Sverige tillgodoses som vi ser det i allt väsentligt av gällande och föreslagna möjligheter för Migrationsverket och Polismyndigheten att använda biometriska uppgifter för att verifiera identitet (se avsnitt 7.4.2 och 7.4.3).

Till det ovan anförda kommer omständigheter hänförliga till sekretess, som enligt vår mening talar mot att låta personer som ansöker om internationellt skydd omfattas av ett identitetsindex. När det gäller uppgifter om bland annat identitet som förekommer i ett ärende om uppehållstillstånd omfattas dessa som utgångspunkt av sekretess, enligt 37 kap. 1 § offentlighets- och sekretesslagen (2009:400). Som exempel på uppgifter som skyddas av bestämmelsen kan nämnas uppgifter om hälsotillstånd och religiös eller politisk uppfattning. Även uppgiften *att* en person har sökt internationellt skydd skyddas.

Uppgifter om medborgarskap kan också medföra risk för den enskilde, om han eller hon kommer från ett land som bedriver flyktingspionage. Personer som ansöker om internationellt skydd kan, som vi ser det, anses mer utsatta i dessa avseenden än den som ansöker om uppehållstillstånd exempelvis på grund av familjeåterförening. Detta påkallar enligt vår bedömning särskild försiktighet, och förutsätter att uppgifterna skyddas på samma sätt i ett identitetsindex som hos Migrationsverket. Vi anser därför att riskerna med att behandla uppgifter om personer som ansöker om internationellt skydd i ett identitetsindex förutsätter att behandlingen kan motiveras av ett mycket tydligt behov av att kunna biometriskt verifiera identitet mot just indexet. Som vi anfört ovan anser vi att ett sådant behov saknas. Nämnda hänsyn till sekretess gör sig normalt gällande endast under tiden en ansökan behandlas; av bestämmelsen i 37 kap. 1 § tredje stycket offentlighets- och sekretesslagen framgår att sekretessen enligt första och andra styckena gäller endast för uppgifter i skälen. Uppgifter om identitet och individnummer framgår av beslutets förstasida, och är därmed som utgångspunkt offentliga.

Vid en sammantagen bedömning av det ovan anförda anser vi att personer som ansöker om internationellt skydd inte bör omfattas av ett identitetsindex.

12.4.3 Personer som vistas olagligen i Sverige

Vår bedömning

Det saknas behov av att personer som vistas olagligen i Sverige omfattas av ett identitetsindex.

I svensk rätt finns inte någon uttrycklig reglering av vad som utgör olaglig vistelse. Det framgår däremot indirekt att med laglig vistelse avses en vistelse som innebär att en utlänning antingen har tillstånd att vistas i landet eller får vistas här medan en ansökan om uppehållstillstånd prövas.[34] En person kan även vistas här med uppehållsrätt eller med visering. I återvändandedirektivet[35] framgår att med olaglig vistelse avses en vistelse på en medlemsstats territorium av en tredje-

[34] *Genomförande av återvändandedirektivet*, prop. 2011/12:60, s. 26.
[35] Europaparlamentets och rådets direktiv 2008/115/EG av den 16 december 2008.

landsmedborgare som inte, eller inte längre, uppfyller de villkor för inresa som anges i EU:s gränskodex eller andra villkor för att resa in, vistas eller vara bosatt i den medlemsstaten. Sammantaget innebär detta att alla tredjelandsmedborgare som inte har laglig rätt att vistas i Sverige vistas här olagligt. Denna krets av personer omfattar därmed som utgångspunkt den som har meddelats ett verkställbart ut- eller avvisningsbeslut. Även den vars avlägsnandebeslut omfattas av inhibition anses vistas olagligen i Sverige.[36]

I många fall skulle det kunna vara så att den som meddelas ett verkställbart ut- eller avvisningsbeslut redan är registrerad i ett identitetsindex, exempelvis genom att han eller hon är eller har varit folkbokförd i landet (se avsnitt 12.3.1). Om den omständigheten att personen inte längre anses vistas i landet lagligen innebär att registreringen ska tas bort, och i så fall vid vilken tidpunkt, återkommer vi till i avsnitt 15.2.2. Detta avsnitt tar i första hand sikte på personer som det inte av annan anledning finns ett behov av att registrera i ett index, och som vistas olagligen i landet. Det kan till exempel vara fråga om någon som har påträffas vid en inre utlänningskontroll och då meddelats ett avvisningsbeslut direkt av Polismyndigheten, eller någon som utvisats av allmän domstol i en brottmålsprocess.

Ett beslut om avvisning eller utvisning ska, enligt 8 kap. 21 § utlänningslagen, i normalfallet innehålla en tidsfrist inom vilken utlänningen frivilligt ska lämna landet. Tidsfristen ska bestämmas till två veckor om utlänningen avvisas och till fyra veckor om han eller hon utvisas. Ett avlägsnandebeslut som inte innehåller någon tidsfrist för frivillig avresa ska verkställas snarast möjligt. Den som har fått ett avlägsnandebeslut är skyldig att lämna Sverige. Det är i första hand alltid den av- eller utvisade som är skyldig att självmant lämna landet och inte svenska myndigheter som är skyldiga att genom tvångsåtgärder verkställa beslutet (jfr MIG 2007:46 och MIG 2008:23). Utgångspunkten är alltså att den som har ett gällande avlägsnandebeslut på eget initiativ ska lämna landet förhållandevis snabbt, och i vart fall inom en sådan tidsram att personen inte kan förväntas etablera en anknytning till landet som innebär att det finns ett behov av att registrera honom eller henne i ett identitetsindex; personen kan varken anses vara bosatt eller ha sin hemvist i Sverige. En person som håller sig undan en verkställighet kan också bli föremål för tvångsåtgärder i form av förvar och uppsikt, i syfte att med tvång

[36] *Inhibition av verkställigheten*, Ds 2024:23, s. 240.

kunna verkställa avlägsnandebeslutet. Även detta talar enligt vår mening mot att personer som vistas olagligen i landet bör omfattas av ett identitetsindex.

Det kan visserligen konstateras att även personer som vistas olagligen i Sverige kan ha rätt till viss sjukvård, skolgång och bistånd.[37] Särskilt avseende skolgång kan det antas att viss anknytning skapas, och i kontakt med sjukvård och sociala myndigheter kan identitet behöva verifieras. Vi anser dock – mot bakgrund av det ovan anförda – att ett sådant behov endast är tillfälligt och inte sådant att det i sig innebär ett behov av att registrera personen i ett identitetsindex. Det kan i detta sammanhang också konstateras att tidigare bestämmelser om preskription – som innebar att ett avlägsnandebeslut upphörde att gälla efter fyra år – har upphävts; enligt 12 kap. 22 § utlänningslagen gäller numera att ett beslut om av- eller utvisning som inte har meddelats av allmän domstol upphör att gälla fem år från det att utlänningen har lämnat landet i enlighet med beslutet. Syftet med denna uppstramning är bland annat att öka incitamentet att följa ett meddelat avlägsnandebeslut.[38] Detta talar som vi ser det ytterligare för att den tid som någon vistas i Sverige olagligen efter ett beslut om av- eller utvisning som utgångspunkt måste ses som tillfällig.

Förslag har lämnats om att Migrationsverket och Polismyndigheten, om det behövs, i ett ärende om avvisning eller utvisning ska få ta upp biometriska underlag och att underlagen ska få lagras i Migrationsverkets register över fingeravtryck och fotografier. Detta skulle kunna tala för att det finns ett behov av att låta även personer som omfattas av förslagen ingå i ett identitetsindex. Det framgår emellertid att syftet med den föreslagna regleringen är att säkerställa att biometriska uppgifter kan registreras i Schengens informationssystem i alla situationer där ett avlägsnandebeslut eller ett återreseförbud ska föras in i systemet.[39] Förslagen har alltså inte någon grund i att dessa personer kan antas vistas i Sverige under någon längre tid.

Mot denna bakgrund anser vi att det saknas ett behov av att personer som vistas olagligen i Sverige omfattas av ett identitetsindex. Om den som omfattas av ett gällande beslut om ut- eller avvisning beviljas uppehållstillstånd är vistelsen emellertid inte

[37] Jfr *Preskription av avlägsnandebeslut och vissa frågor om återreseförbud*, SOU 2024:10, s. 45 ff. och Ds 2024:23, kapitel 4.
[38] SOU 2024:10, s. 124.
[39] *Stärkt återvändandeverksamhet*, prop. 2025/26:263, s. 123 ff. och 159. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.

längre att betrakta som olaglig, och om giltighetstiden för uppehållstillståndet överstiger ett år kan ett behov av att omfattas av ett index finnas av den anledningen (se avsnitt 12.3.3).

12.4.4 Personer som har beviljats visering

Vår bedömning

Det saknas behov av att låta personer som har beviljats en visering omfattas av ett identitetsindex.

En Schengenvisering eller nationell visering kan beviljas för att möjliggöra en kortare vistelse i Sverige; Schengenviseringen kan beviljas för högst 90 dagar under en 180-dagarsperiod, enligt artikel 1.1 i viseringskodexen[40] och en nationell visering får ha en giltighetstid om högst ett år, enligt 3 kap. 6 § utlänningslagen. Syftet med en visering är alltså normalt sett att möjliggöra kortare besök, exempelvis för att resa som turist eller för att besöka en konferens. En nationell visering får beviljas endast om det finns särskilda skäl (3 kap. 4 § utlänningslagen). I förarbetena nämns som exempel på särskilda skäl att det rör sig om nära släktingar som önskar vistas i Sverige längre tid än tre månader eller att det kan vara fråga om affärsbesök. I sådana fall ansöker utlänningen dock ofta i stället om uppehållstillstånd för besök. Vidare kan det röra sig om att det finns praktiska hinder som gör att det inte är möjligt att utfärda ett uppehållstillstånd innan inresa. En sådan situation kan uppstå vid uttagning av så kallade kvotflyktingar.[41]

Sammantaget är det alltså fråga om personer som kan förväntas vistas i Sverige under en relativt kort tid och som inte kommer att arbeta eller bosätta sig i landet. Det kan därmed inte antas att det finns behov av att kunna verifiera deras identitet mot ett identitetsindex under vistelsen. För att beviljas visering krävs också styrkt identitet och innehav av en giltig passhandling. Det kan därför antas att deras identitet vid behov kan verifieras genom kontroll av passhandlingen och av de uppgifter som finns registrerade i den centrala utlänningsdatabasen och relevanta EU-gemensamma informations-

[40] Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009.
[41] *EU:s viseringskodex*, prop. 2010/11:121 s. 36 och *Ny instans- och processordning i utlännings- och medborgarskapsärenden*, prop. 2004/05:170, s. 272 f.

system. Det saknas alltså ett behov av att låta personer som har beviljats visering omfattas av ett identitetsindex. Om personen ansöker om uppehållstillstånd under vistelsen i Sverige och beviljas ett sådant kan ett behov då i stället uppkomma, om uppehållstillståndets giltighetstid överstiger ett år.

12.4.5 Personer med uppehållsrätt som saknar en identitetsbeteckning

Vår bedömning

Det saknas behov av att personer som under begränsad tid vistas i Sverige med stöd av regelverket om fri rörlighet och som saknar en identitetsbeteckning och inte beviljats uppehållstillstånd med en giltighetstid om minst ett år omfattas av ett identitetsindex.

Det EU-rättsliga regelverket om fri rörlighet[42] ger en omfattande rätt för EES-medborgare och deras familjemedlemmar att resa in i och vistas i Sverige och andra medlemsstater, bland annat för att arbeta, studera, söka jobb eller starta egen verksamhet. EES-medborgare har som utgångspunkt en rätt att vistas i Sverige i högst tre månader under förutsättning att personen kan identifiera sig med pass eller annan id-handling. För en rätt att vistas i landet i mer än tre månader krävs att EES-medborgaren uppfyller villkoren för uppehållsrätt, till exempel genom att personen är arbetstagare, egenföretagare eller student som är inskriven vid en erkänd utbildningsanstalt. Detta framgår av 3 a kap. 3 § utlänningslagen. Uppehållsrätten inträder automatiskt och gäller så länge villkoren är uppfyllda. Det sker därför inte någon föregående prövning av frågan om uppehållsrätt (jfr 3 a kap. 5 § utlänningslagen), vilket innebär att det kan vara svårt att vid en viss given tidpunkt dra någon säker slutsats om hur länge personen kan antas komma att vistas i Sverige.

För att åstadkomma en ansvarsfull, stram och hållbar migrationspolitik är det enligt regeringen viktigt att svenska myndigheter får kännedom om och kan kontrollera EES-medborgares vistelse och uppehållsrätt i landet i större utsträckning än i dag, då registrering av dessa personer sker endast vid folkbokföring och vid tilldelning

[42] Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004.

av samordningsnummer. I betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* lyftes bland annat fram att multipla identiteter kan uppkomma exempelvis genom att en person hos Skatteverket har folkbokförts som EES-medborgare (vilket sker utan att Migrationsverket har kontakt med individen) samtidigt som denne hos Migrationsverket har sökt och beviljats uppehållstillstånd som icke EES-medborgare.[43] Riksrevisionen har i rapporten *Vem där – fastställande av identitet vid statliga myndigheter* pekat på att brister i processerna för att säkerställa att identitetsuppgifterna i folkbokföringsverksamheten är korrekta och unika blir särskilt allvarliga när det gäller EES-medborgare, då Skatteverket oftast är den första och enda myndighet som fastställer en grundidentitet för dessa personer.[44] I betänkandet *Registrering av EES-medborgare* har förslag lämnats om att EES-medborgare som vistas i Sverige i över tre månader som huvudregel ska vara registreringsskyldiga. Enligt förslagen ska Migrationsverket ha möjlighet att ta fotografi och fingeravtryck i ärenden om registrering av uppehållsrätt och att ta fram biometriska uppgifter ur dessa, för att kontrollera identitet mot uppgifterna i EES-medborgarens pass eller identitetskort.[45]

Ovan nämnda problem med multipla identiteter är enligt vår mening hänförliga till situationer när den som vistas i Sverige med stöd av reglerna om fri rörlighet ska folkbokföras efter flyttning till landet, tilldelas ett samordningsnummer eller beviljas ett uppehållstillstånd i Sverige. Som en följd av våra bedömningar i avsnitt 12.3.1–12.3.3 kommer en EES-medborgare och eventuella familjemedlemmar som vistas i landet med (härledd) uppehållsrätt att kunna omfattas av personkretsen för ett identitetsindex vid folkbokföring, tilldelning av samordningsnummer och beviljande av uppehållstillstånd med en giltighetstid som överstiger ett år. I det ovan nämnda betänkandet om registrering av EES-medborgare föreslogs att Migrationsverket ska utfärda ett registreringsbevis till registrerade EES-medborgare och i samband med det begära ett samordningsnummer hos Skatteverket, om EES-medborgaren inte är eller har varit folkbokförd eller redan har tilldelats ett samordningsnummer.[46] Enligt förslaget ska EES-medborgare som vistas i Sverige längre tid än tre månader med uppehållsrätt, och som inte redan har en identitetsbeteckning, alltså

[43] SOU 2025:75, s. 490.
[44] RiR 2024:12, s. 5.
[45] SOU 2026:9, s. 119 och 194 ff.
[46] SOU 2026:9, s. 119 och 170.

tilldelas ett samordningsnummer och kan i samband med det registreras i ett identitetsindex, om biometriska underlag tas upp i samband med tilldelningen. Att en person med uppehållsrätt vistas i landet längre än tre månader innebär som vi ser det emellertid inte nödvändigtvis i sig att han eller hon också har en sådan anknytning till landet att det finns ett behov av att verifiera personens identitet mot ett identitetsindex. Att uppehållsrätten upphör så fort förutsättningarna inte längre är uppfyllda talar också för att det bör krävas viss tidsmässig stabilitet i uppehållsrätten och därmed anknytningen till landet för att dessa personer ska omfattas av personkretsen för identitetsindexet. Sådan anknytning uppkommer enligt vår bedömning inte nödvändigtvis genom en registrering av uppehållsrätten utan snarast genom att personen folkbokförs, tilldelas ett samordningsnummer eller beviljas uppehållstillstånd i Sverige.

Mot denna bakgrund anser vi att det inte finns behov av att EES-medborgare samt familjemedlemmar till dessa som vistas i Sverige med stöd av regelverket om rätt till fri rörlighet och som inte folkbokförs, tilldelas ett samordningsnummer eller beviljas uppehållstillstånd omfattas av ett identitetsindex.

12.4.6 Diplomatisk personal

Vår bedömning

Det saknas behov av att diplomatisk personal och personer som tillhör en främmande stats militära styrka eller ett Natohögkvarter och som vistas i Sverige omfattas av ett identitetsindex.

Av 2 och 3 §§ lagen (1976:661) om immunitet och privilegier i vissa fall följer att främmande stats beskickning och beskickningsmedlemmar och deras familjer och betjäning samt diplomatiska kurirer åtnjuter immunitet och privilegier enligt 1961 års Wienkonvention om diplomatiska förbindelser. På samma sätt åtnjuter främmande stats konsulat och konsulatsmedlemmar, deras familjer och betjäning samt konsulära kurirer immunitet och privilegier enligt 1963 års Wienkonvention om konsulära förbindelser.

Vad immuniteten och privilegierna närmare består i framgår av respektive konvention. I båda traktat är utgångspunkten dock att

beskicknings- och konsulatsmedlemmar har kvar en sådan stark anknytning till sina hemländer att de i folkrättslig mening inte anses vara stadigvarande bosatta i landet de är utsända till, trots att de i en mer allmän bemärkelse faktiskt bor där och kan göra det under flera år.[47] Den som tillhör en främmande makts beskickning eller lönade konsulat eller dess betjäning samt den som tillhör en främmande stats militära styrka eller ett Natohögkvarter ska därför, enligt 4 § andra stycket och 5 och 5 a §§ folkbokföringslagen, som huvudregel inte folkbokföras trots att kraven för folkbokföring enligt 3 § och 4 § första stycket folkbokföringslagen är uppfyllda. Dessa personer har i förarbetena ansetts ha så svag anknytning till det svenska samhället att det är olämpligt att folkbokföra dem.[48] En sådan anställning medför enligt praxis på utlänningsrättens område normalt inte heller att det finns en sådan anknytning till Sverige att uppehållstillstånd beviljas om anställningen upphör (se MIG 2009:33). Reglerna innebär vidare att den som vistas här med diplomatisk immunitet inte förvärvar hemvist enligt medborgarskapslagen (jfr RÅ 1972 ref. 35).

Personer med anknytning till utländska beskickningar och karriärkonsulat – dock ej lokalanställda – samt personer som tillhör en främmandes stat militära styrka eller ett Natohögkvarter anses alltså varken vara bosatta eller ha hemvist i Sverige. I ärenden om uppehållstillstånd har de inte heller ansetts ha en särskild anknytning till Sverige genom anställningen. De är enligt 2 kap. 10 § utlänningslagen vidare undantagna krav på pass, visering, uppehållstillstånd och arbetstillstånd. Dessa omständigheter talar enligt vår mening sammantaget mot att det finns ett behov av att registrera dessa personer i ett identitetsindex.

I motsatt riktning talar däremot att även den som tillhör en främmande makts beskickning eller lönade konsulat eller dess betjäning får tilldelas ett personnummer, enligt 18 b § folkbokföringslagen, om personen har rätt att vistas i landet och uppfyller de förutsättningar som anges i 3 § första stycket. Personnumret används i kontakter med myndigheter och andra aktörer, i situationer där identiteten vanligtvis behöver verifieras. Möjligheten att tilldela diplomatiska företrädare personnummer trots att de inte folkbokförs har motiverats bland annat med att det underlättar deras vardagliga liv i Sverige.

[47] *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 120 f.
[48] *Folkbokföring av personer med anknytning till internationella organ*, prop. 2009/10:245, s. 10.

Dessa personnummer har emellertid i vissa situationer upplevts inte ha riktigt samma gångbarhet i samhället som en folkbokförd persons personnummer.[49] Det kan här noteras att det i förarbetena till lagen om samordningsnummer uttalades att den som tilldelas ett personnummer har en mycket stark anknytning till Sverige.[50] Detta uttalande kan dock, enligt vår mening, inte anses ha någon direkt bäring på den särskilt utpekade personkrets som framgår av 5 och 5 a §§ folkbokföringslagen.

En folkbokföring av diplomatiska företrädare har bedömts kunna strida mot allmänna internationella principer för hur dessa personer ska hanteras av den mottagande staten.[51] Trots att dessa personer inte ska folkbokföras får ett personnummer, som vi angett ovan, fastställas för dem om förutsättningarna för folkbokföring i övrigt är uppfyllda (18 b § folkbokföringslagen). Diplomatiska företrädare kan också tilldelas samordningsnummer på begäran av Försvarsmakten eller Regeringskansliet i vissa fall, i enlighet med 4 § förordningen (2023:363) om samordningsnummer. Att registrera biometriska uppgifter för diplomatiska företrädare i ett identitetsindex skulle enligt vår bedömning riskera att hamna i konflikt med internationella principer. Vi kan i detta sammanhang även notera att kravet på personlig inställelse i 2 kap. 2 § lagen om samordningsnummer inte gäller för en person som omfattas av lagen om immunitet och privilegier i vissa fall. Skyldigheten enligt 26 § folkbokföringslagen att anmäla flyttning till Sverige gäller inte heller för dessa personer (se bestämmelsens tredje stycke). Dessa personer omfattas alltså inte heller av kravet på personlig inställelse i folkbokföringslagen. Denna personkategori förekommer därmed inte i denna typ av ärendeslag där biometriska underlag kan tas upp.

I egenskap av utländska medborgare kan de inte heller ansöka om ett svenskt pass eller ett nationellt identitetskort. Ett sådant statligt identitetskort som föreslagits i promemorian *Ett statligt identitetskort* ska dock kunna utfärdas bland annat till utlänningar som har tilldelats ett personnummer enligt 18 b § folkbokföringslagen och som omfattas av lagen om immunitet och privilegier i vissa fall och till utlänningar som efter att ha styrkt sin identitet har tilldelats ett

[49] Prop. 2009/10:245, s. 10 och *Personnummer och samordningsnummer*, prop. 2008/09:111, s. 34.
[50] Prop. 2021/22:276, s. 41.
[51] Prop. 2009/10:245, s. 10.

samordningsnummer enligt lagen om samordningsnummer, och numret inte är förklarat vilande[52].

Även med hänsyn till att personer med anknytning till utländska beskickningar och karriärkonsulat, och personer som tillhör en främmandes stat militära styrka eller ett Natohögkvarter, kan vistas stadigvarande i Sverige och att det då kan finnas att behov för svenska myndigheter att biometriskt verifiera deras identitet, anser vi sammantaget att det inte finns ett behov av att registrera dem i ett identitetsindex. Deras särskilda ställning och därtill följande immunitet och privilegier har då särskilt beaktats.

[52] Ju2026/01595, s. 7.

13 Registrering av en identitetsnyckel

13.1 Inledning

Vi har tidigare bedömt att befintliga uppgifter om identitet i de register som förs av Migrationsverket, Polismyndigheten och Skatteverket inte bör föras över till ett nytt identitetsindex, utan att ett sådant index bör byggas upp från grunden (se avsnitt 10.7.6). Det innebär att vi behöver ta ställning till när och för vem en registrering i indexet bör göras och en identitetsnyckel skapas.

I kapitel 12 har vi redogjort för vilka behov som finns – respektive inte finns – av att låta ett identitetsindex omfatta olika personkategorier. I det här kapitlet utvärderar vi i vilka situationer en person bör registreras i ett index, med beaktande av bland annat befintligt regelverk avseende möjligheter att ta upp biometriska underlag.

13.2 Utgångspunkter

13.2.1 Kontroll av om en individ är registrerad i ett identitetsindex

Vår bedömning

Innan en identitetsnyckel kan skapas i ett identitetsindex måste en kontroll av den aktuella personens biometriska uppgifter göras mot indexet för att säkerställa att personen inte redan är registrerad.

En grundförutsättning för att ett identitetsindex ska fylla sin funktion är att endast unika identiteter registreras. Om en myndighet möter en person i en situation som enligt vår bedömning bör utgöra

grund för registrering i ett index behöver myndigheten kontrollera om personen är registrerad i indexet sedan tidigare, för att kunna avgöra om en identitetsnyckel ska skapas eller inte.

Ett första steg i denna kontroll är att myndigheten söker mot systemet med de alfanumeriska uppgifter som personen i fråga uppger för myndigheten, vanligtvis ett personnummer. En identitetsnyckel kan givetvis också användas för sökningen om personen gör en sådan tillgänglig. Om en sådan sökning i ett index ger en träff kan personens identitet kontrolleras genom en biometrisk verifiering, det vill säga genom att de biometriska underlag som har tagits upp i någon av de situationer som vi redogör för i avsnitt 13.3 jämförs med de biometriska uppgifter som är kopplade till träffen i indexet. Om identiteten kan verifieras på detta sätt bekräftas att personen redan är registrerad i indexet. En identitetsnyckel ska då inte skapas.

Om en persons uppgivna identitet inte kan verifieras mot uppgifter i identitetsindexet behöver myndigheten göra en en-till-många-jämförelse med hjälp av biometriska uppgifter, för att klarlägga att individen inte förekommer i indexet med någon annan identitet. För det fall en sådan identifiering ger en träff på en redan registrerad individ kan utredningsåtgärder behöva vidtas. Vi återkommer till frågan om uppdatering och rättelse av registrerade uppgifter i ett index i kapitel 14. Oavsett vilka åtgärder som eventuellt behöver vidtas innebär en träff efter en identifiering att en identitetsnyckel inte ska skapas för personen i fråga. Om en verifiering eller identifiering med biometriska uppgifter inte ger någon träff i identitetsindexet, och personen alltså inte redan förekommer, kan personen registreras och en identitetsnyckel skapas för honom eller henne.

Våra bedömningar i det här kapitlet utgår från att personen i fråga inte redan är registrerad i ett identitetsindex. En person som till exempel registreras i samband med flyttning till och folkbokföring i Sverige ska alltså inte tilldelas en ny identitetsnyckel om han eller hon senare beviljas svenskt medborgarskap. Däremot ska en person som inte tidigare förekommer i ett identitetsindex, enligt våra bedömningar, tilldelas en identitetsnyckel i samband med att han eller hon beviljas svenskt medborgarskap. Undantaget från denna huvudregel om ”en person en identitet” är personer som tilldelas en kvalificerad skyddsidentitet och, enligt vår bedömning (se avsnitt 13.3.8), i samband med det bör registreras i ett identitetsindex och få en identitetsnyckel kopplad till skyddsidentiteten.

13.2.2 Kontroll av eventuell sekretessmarkering

Vår bedömning

När en identitetsnyckel skapas för en person behöver det kontrolleras om han eller hon har en sekretessmarkering i folkbokföringen. Om så är fallet bör en sådan markering göras för personen även i identitetsindexet.

Vi har i avsnitt 11.4.6 bedömt att ett identitetsindex bör innehålla en notering om att en viss individ har en sekretessmarkering i folkbokföringsverksamheten. Detta är viktigt för att en uppgift om personens namn inte felaktigt ska lämnas ut vid en verifiering av identitet mot ett index. När en identitetsnyckel skapas måste därför den myndighet som skapar nyckeln kontrollera om personen har en sekretessmarkering i folkbokföringen. Detta framgår av Navet, Skatteverkets system för distribution av folkbokföringsuppgifter till samhället, som de myndigheter som bör kunna skapa en identitetsnyckel har tillgång till. Vi anser inte att den myndighet som skapar en identitetsnyckel ska göra en egen bedömning av om en markering bör föras in även i ett index i det enskilda fallet, utan en sekretessmarkering i folkbokföringen bör motsvaras av en sådan markering i ett index.

Hur kontrollen bör gå till i praktiken anser vi inte behöver regleras närmare. Det kan ske antingen genom en manuell kontroll eller genom att systemet med ett identitetsindex gör en automatisk kontroll mot Navet och då – utan någon manuell hantering – för in en markering i indexet när en identitetsnyckel skapas, om personen har en sekretessmarkering i folkbokföringen. Det bör tydliggöras att en kontroll av förekomsten av en sekretessmarkering i folkbokföringen endast bör göras när en identitetsnyckel faktiskt skapas.

13.2.3 Inget beviskrav avseende identitet

Vår bedömning

Det bör inte ställas upp ett visst beviskrav avseende en persons identitet som ska vara uppfyllt för att han eller hon ska kunna registreras i ett identitetsindex.

Vi har tidigare bedömt att det faktum att ett visst beviskrav avseende identiteten i ett ärende är uppfyllt inte automatiskt innebär att identiteten är verifierad (avsnitt 7.2.2). Behov av att kunna verifiera en persons identitet kan uppstå i en mängd olika ärenden och situationer. Vilket beviskrav som gäller i ett ärende och om det är uppfyllt eller inte kan, enligt vår mening, emellertid ändå vara av betydelse när myndigheten avgör om det finns ett behov av att verifiera den enskildes identitet genom kontroll – av biometriska uppgifter – mot ett identitetsindex.

Under arbetets gång har vi stött på uppfattningen att en identitetsnyckel bör kunna skapas endast när personen i fråga har styrkt sin identitet med en godtagbar identitetshandling. Det är givetvis av värde att korrekta identitetsuppgifter registreras i ett identitetsindex och kopplas till en identitetsnyckel. Enligt vår mening kan dock registrering i ett index av personer med osäker eller sannolik identitet – för att använda samma terminologi som vid tilldelning av samordningsnummer – fylla en viktig funktion.

Vad gäller en svensk medborgare som varit folkbokförd och bosatt i Sverige sedan födelsen och som vid personlig inställelse kan identifiera sig med ett svenskt pass kan det i många fall antas saknas behov av verifiering mot ett index. Om endast personer som kan styrka sin identitet med en godtagbar identitetshandling ska kunna registreras i ett identitetsindex skulle ett sådant system, enligt vår bedömning, fylla en mer begränsad funktion än nödvändigt. Vi anser i stället att behovet av att kunna verifiera identitet genom kontroll mot ett index kan vara som störst i situationer där en persons identitet är oklar, när personen saknar godtagbara identitetshandlingar för att kunna styrka sin identitet eller när det finns anledning att ifrågasätta för vem åberopade handlingar är utfärdade. Som exempel kan nämnas en tredjelandsmedborgare som tilldelats ett samordningsnummer med osäker identitet och åberopar detta nummer vid kontakt med

en myndighet. I en sådan situation kan det generellt sett antas finnas ett behov av verifiering mot ett index.

Mot den här bakgrunden anser vi att en person bör kunna registreras i ett identitetsindex oberoende av vilket beviskrav som är tillämpligt i det ärende som aktualiserat registreringen, och oberoende av om detta beviskrav ansetts vara uppfyllt. Vidare bedömer vi att det inte heller bör ställas upp något särskilt beviskrav avseende en persons identitet för att han eller hon ska kunna registreras i ett index. Som vi påpekat ovan är det framför allt för personer som inte kan styrka sin identitet som det finns ett behov av att kunna verifiera identiteten mot uppgifter i ett identitetsindex.

Genom att en identitetsnyckel skapas först efter att det har säkerställts att personen inte redan förekommer i indexet (se avsnitt 13.2.1) ska en person kunna tilldelas endast en identitetsnyckel, till vilken personens biometriska uppgifter är kopplade. Även om identitetsuppgifter som en identitetsnyckel är kopplade till – exempelvis namn – skulle kunna vara felaktiga, finns det möjlighet att verifiera att personen som myndigheten möter är samma person som tilldelats den aktuella identitetsnyckeln. En person som är registrerad i ett index kan alltså endast agera i den registrerade identiteten – som möjligen är felaktig – och inte uppträda som någon annan, när han eller hon kommer i kontakt med en myndighet som verifierar identitet genom kontroll av biometriska uppgifter mot indexet. Därmed fyller även en identitetsnyckel som kopplats till icke styrkta, eventuellt även felaktiga, identitetsuppgifter en funktion.

13.2.4 Registrering i samband med att biometriska underlag tas upp vid handläggningen av ett ärende

Vår bedömning

Registrering av en person i ett identitetsindex bör kunna göras endast när en myndighet i samband med handläggningen av ett ärende tar upp biometriska underlag.

Ju fler personer som är registrerade i ett identitetsindex desto större nytta skulle det rimligen kunna få. Det är därmed naturligt att sträva efter att samtliga de personer vars identitet kan behöva verifieras

vid kontakt med myndigheter registreras i ett index så snart som möjligt. För att kunna ta upp biometriska underlag och registrera personer i ett index, utan koppling till befintlig ärendehantering eller annan verksamhet hos en myndighet, skulle emellertid en helt ny process behöva införas, vars huvudsakliga syfte är att skapa en identitetsnyckel. Det är enligt vår mening inte lämpligt, av flera olika anledningar.

Till att börja med bör det, enligt vår bedömning, inte föreligga något tvång för en person att registreras i ett index enbart för att han eller hon tillhör en personkrets som det kan antas finnas ett behov av att verifiera identitet för, till exempel en person som är folkbokförd i Sverige. Att tvinga en mycket stor andel av den svenska befolkningen att personligen inställa sig hos en myndighet enbart för att biometriska underlag ska kunna tas upp och biometriska uppgifter registreras i ett index är, enligt vår mening, inte proportionerligt i förhållande till fördelen med att relativt snabbt kunna bygga upp ett omfattande register.

Vidare gynnas ett system med ett identitetsindex av att en identitetsnyckel, och de biometriska uppgifterna, kopplas till korrekta identitetsuppgifter. Det innebär att den myndighet som möter personen i fråga och vars utredning ligger till grund för en registrering i ett index bör göra någon form av identitetskontroll i samband med att biometriska underlag tas upp och en person ska registreras. Vi anser att det är att föredra att en sådan kontroll utförs inom ramen för ett annat ärende eller annan verksamhet hos aktuell myndighet – där sådan kontroll ska göras oberoende av om personen i fråga har en identitetsnyckel – än specifikt i ett ärende om registrering i ett index. Man kan i sådant fall utnyttja de rutiner och ta till vara den kompetens som finns hos den aktuella myndigheten i det andra ärendeslaget eller den andra verksamheten. Det bör även beaktas att en helt separat process för upptagning av biometriska underlag och identitetskontroll, enbart i syfte att skapa en identitetsnyckel, kan komma att ta större resurser i anspråk. Det finns alltså en fördel med att samordna registreringen av personer i ett identitetsindex med handläggningen av andra ärenden eller annan verksamhet.

Det är enligt vår mening också en fördel att myndigheters möjligheter att ta upp biometriska underlag inte utökas mer än nödvändigt. Genom att skapa ett system med ett identitetsindex med utgångspunkt i myndigheters befintliga – och föreslagna – möjligheter att

ta upp biometriska underlag begränsas påverkan på den personliga integriteten. Biometriska underlag som tas upp av Skatteverket vid till exempel inflyttning till Sverige skulle på så sätt kunna användas både i Skatteverkets folkbokföringsverksamhet och i ett identitetsindex, i stället för att den enskilde behöver lämna sådana underlag vid flera tillfällen, potentiellt hos flera olika myndigheter.

Att skapa en identitetsnyckel i samband med handläggningen av ett ärende där den enskilde ansöker om till exempel pass eller statligt identitetskort skulle kunna få en avhållande effekt. Att någon registreras i ett identitetsindex kan emellertid, som vi ser det, inte anses medföra några faktiska betungande verkningar för den enskilde, utöver att biometriska uppgifter och andra personuppgifter lagras och behandlas även i ett annat sammanhang än det för vilket de biometriska underlagen primärt togs upp. Det medför inga ytterligare kostnader eller skyldigheter för den enskilde och bör enligt vår bedömning uppfattas inte enbart som en utökad kontroll från det allmännas sida utan som en skyddsmekanism för enskilda, genom det utökade skydd mot att andra uppträder i din identitet som ett index främjar.

Mot den här bakgrunden bedömer vi att registrering av en person i ett identitetsindex bör kunna göras endast när en myndighet i samband med handläggningen av ett ärende tar upp biometriska underlag.

Särskilt om fakultativa bestämmelser

Vi har ovan bedömt att registrering av en person i ett identitetsindex bör kunna göras endast när en myndighet i samband med handläggningen av ett ärende tar upp biometriska underlag; registrering i ett index bör alltså inte utgöra ett eget, särskilt, ärende. I vissa relevanta bestämmelser som reglerar myndigheters möjligheter att använda biometri *ska* myndigheten ta upp biometriska underlag, medan det i andra bestämmelser anges att myndigheten *får* ta upp sådana underlag. Som exempel kan nämnas den föreslagna bestämmelsen i 13 f § lagen (2001:82) om svenskt medborgarskap, medborgarskapslagen. Enligt bestämmelsen får Migrationsverket fotografera en utlänning som har uppehållstillstånd och, om han eller hon har fyllt sex år, ta hans eller hennes fingeravtryck i vissa ärenden om medborgarskap.[1] I vissa situationer – i vilka vi enligt bedömningarna nedan anser att

[1] *Stärkt återvändandeverksamhet*, prop. 2025/26:263, s. 8 och 129 ff.

en registrering i ett identitetsindex som utgångspunkt *ska* göras om den enskilde inte redan har en identitetsnyckel – kan myndigheten i fråga alltså bedöma att biometriskt underlag inte ska tas upp. Om myndigheten i en sådan situation väljer att inte ta upp biometriska underlag ska en identitetsnyckel, enligt vår bedömning, inte skapas, trots att förutsättningarna i övrigt för en registrering är uppfyllda. Det får visserligen anses ligga i vårt uppdrag att utforma ett system med ett identitetsindex på ett sådant sätt att det kan få ett tillräckligt genomslag. Vi bedömer dock att det inte är möjligt eller lämpligt att – endast i syfte att möjliggöra att fler personer registreras i ett index – förändra myndigheternas bedömningsutrymme avseende när biometriska underlag tas upp i befintliga ärendeslag, genom att införa en genomgående skyldighet att ta upp sådana underlag. Det saknas anledning att ha någon annan utgångspunkt än att myndigheterna faktiskt tar upp biometriska underlag när detta behövs och är möjligt i aktuella ärendeslag.

Våra bedömningar i det här kapitlet utgår därmed från att myndigheten i fråga har ett rättsligt stöd i verksamhetsspecifikt regelverk för att ta upp biometriskt underlag och faktiskt också gör det.

13.2.5 Registrering på frivillig basis

Vår bedömning

Det bör inte finnas en möjlighet för enskilda att på frivillig basis bli registrerade i ett identitetsindex och få en identitetsnyckel.

Skapandet av en identitetsnyckel och lagringen av biometriska uppgifter om en person i ett identitetsindex innebär ett intrång i den personliga integriteten (se kapitel 17). En identitetsnyckel kan dock medföra ett skydd för den enskilde och förhindra att dennes uppgifter och identitet utnyttjas av någon annan, med den enskildes uppgifter som underlag.[2] Man kan därför tänka sig att det kommer att finnas personer som skulle vilja bli registrerade i ett identitetsindex och få en identitetsnyckel. En möjlighet för enskilda att registreras på eget initiativ skulle också potentiellt gynna en snabbare uppbyggnad av ett index. Med anledning av det behöver vi utvärdera

[2] Jfr *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 458.

om det bör finnas en möjlighet att bli registrerad i ett index på frivillig basis.

Som vi har kommit fram till ovan finns det fördelar med att en person registreras i ett index endast i samband med att en myndighet – Migrationsverket, Polismyndigheten eller Skatteverket (se avsnitt 13.4) – tar upp biometriska underlag i samband med handläggningen av ett ärende. De omständigheter vi redogjort för i avsnitt 13.2.4 gör sig gällande även i det nu aktuella avseendet.

Vid ställningstagande till registrering på frivillig basis behöver det också beaktas att det inledningsvis skulle kunna bli ett mycket högt tryck från allmänheten. En myndighet som skulle komma att få i uppgift att ta upp biometriska underlag från personer som på eget initiativ vill registrera sig i ett identitetsindex kan i så fall behöva organisera ett mer storskaligt mottagande. Det kan också antas behövas ett bokningssystem liknande det Polismyndigheten har för utfärdande av pass, vilket för med sig kostnader. Det skulle också kunna antas bli en begränsad tidsvinst i flera situationer. Som exempel kan nämnas en person som väljer att registrera sig frivilligt i ett index, för att några månader senare ansöka om ett nytt pass och i och med det ändå registreras, om än något senare. Dessutom finns det för svenska medborgare – det vill säga en mycket stor andel av de personer som enligt vår bedömning bör omfattas av ett identitetsindex – också en möjlighet att, så att säga, tidigarelägga en registrering i indexet. Svenska medborgare kan nämligen ansöka om pass, både när medborgaren inte har en sådan handling sedan tidigare och innan giltighetstiden för ett utfärdat pass har gått ut. I samband med det skulle medborgaren registreras i ett index och tilldelas en identitetsnyckel, om denne inte redan har registrerats (se avsnitt 13.3.2). För personer som inte är svenska medborgare men som är folkbokförda i Sverige kommer motsvarande möjlighet att finnas vad gäller det statliga identitetskort som föreslagits i promemorian *Ett statligt identitetskort*[3] (se avsnitt 13.3.3). Ett sådant tillvägagångssätt medför visserligen en kostnad för den enskilde, men kostnaden är relativt liten. Det framstår också som rimligt att ta ut en avgift för frivillig registrering i ett index om en sådan möjlighet skulle införas, varför det inte skulle bli någon större skillnad kostnadsmässigt för den enskilde.

Ett annat skäl mot registrering i ett identitetsindex på frivillig basis är att det enligt vår bedömning är olämpligt att tillämpa den

[3] Ju2026/01595.

rättsliga grunden samtycke när en identitetsnyckel skapas. Samtycke från den registrerade kan utgöra rättslig grund för att behandla personuppgifter och ett tillämpligt undantag från förbudet mot att behandla känsliga personuppgifter. Detta framgår av artikel 6.1 a och 9.2 a i dataskyddsförordningen[4]. Samtycke definieras i artikel 4.11 som varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne. Om behandlingen grundar sig på samtycke enligt artikel 6.1 a eller 9.2 a föreligger en rätt för den registrerade att när som helst återkalla sitt samtycke, utan att det påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades (artikel 7.3). Den registrerade ska, enligt artikel 13.2 c och 14.2 d, informeras om att samtycket kan återkallas. För att säkerställa att ett samtycke till personuppgiftsbehandling har lämnats frivilligt bör samtycke, enligt skäl 43 till dataskyddsförordningen, inte utgöra rättslig grund för behandling av personuppgifter där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Europeiska dataskyddstyrelsen (EDPB) anför i riktlinjer om samtycke att det finns andra rättsliga grunder som i princip är mer lämpliga för myndigheters verksamhet.[5] Redan den omständigheten att de biometriska uppgifterna i ett identitetsindex skulle behandlas av en myndighet talar alltså mot att samtycke är en lämplig rättslig grund enligt artikel 6.1 eller grund för undantag enligt artikel 9.2 a i dataskyddsförordningen.

Vidare finns det enligt vår bedömning en konkret risk att ett system med ett identitetsindex, som bygger på samtycke från enskilda, skulle komma att innehålla uppgifter om endast en del av de personer som enligt vår bedömning bör omfattas av systemet (se kapitel 12). Det är enligt vår mening nämligen rimligt att anta att ett inte obetydligt antal personer inte frivilligt – på det sätt som avses i artikel 4.11 i dataskyddsförordningen – kommer att lämna samtycke till behandling av personuppgifter i ett identitetsindex, i synnerhet vad gäller biometriska uppgifter. En annan betydelsefull omständighet

[4] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[5] EDPB, *Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679*, s. 8.

är att ett samtycke till behandling kan återkallas av den enskilde när som helst. Det innebär i praktiken att ett identitetsindex funktion för att verifiera identitet skulle vara avhängig av den enskildes kontinuerliga samtycke till en sådan åtgärd, vilket inte är lämpligt.

Vi ser det inte heller som ett alternativ att införa en möjlighet till frivillig registrering i indexet endast för vissa personkategorier. Dels är det problematiskt att i författning specificera vilka personer som ska ha möjlighet att registrera sig frivilligt, dels kan det antas medföra svårigheter för en myndighet som ska ta upp biometriska underlag – och skapa en identitetsnyckel – att avgöra om personen i fråga tillhör den specificerade personkretsen. Det bör enligt vår mening inte finnas något direkt utrymme för bedömning av om en person ska registreras eller inte.

Sammantaget anser vi att övervägande skäl talar för att det inte bör finnas en möjlighet för den enskilde att på frivillig basis bli registrerad i ett identitetsindex och få en identitetsnyckel.

13.2.6 En möjlighet för andra myndigheter än Skatteverket, Migrationsverket och Polismyndigheten att initiera en registrering i ett identitetsindex

Vår bedömning

Registrering av en person i ett identitetsindex bör inte kunna initieras av andra aktörer än Skatteverket, Migrationsverket och Polismyndigheten.

Vid införande av ett system med ett identitetsindex i enlighet med våra bedömningar kommer berörda myndigheter, i vart fall inledningsvis, att i relativt stor utsträckning möta personer som ännu inte har registrerats i indexet. Dessa personers identitet kommer därmed inte att kunna verifieras genom kontroll av biometriska uppgifter i indexet. Eftersom en sådan verifiering är mycket säkrare än till exempel en okulär kontroll av en fysisk identitetshandling kan man tänka sig att den aktuella myndigheten ser ett behov av att personen i fråga registreras i indexet. I avsnitt 13.3 bedömer vi att en identitetsnyckel bör kunna skapas i samband med Skatteverkets, Migrationsverkets och Polismyndighetens handläggning av vissa ärendeslag.

Fråga är om det bör finnas en möjlighet för andra aktörer än dessa myndigheter att initiera en registrering av en person i ett index.

En jämförelse kan göras med systemet med samordningsnummer, som vi redogör för nedan i avsnitt 13.3.7. Här kan påpekas att för det fall den enskilde inte medverkar när en myndighet begär tilldelning av samordningsnummer och inte inställer sig personligen för identitetskontroll när Skatteverket begär det kan samordningsnummer ändå tilldelas på identitetsnivå sannolik och i vissa fall osäker.[6] Registrering av en person i ett identitetsindex förutsätter i samtliga fall att biometriskt underlag kan tas upp av personen i fråga. Till skillnad från vid tilldelning av samordningsnummer på identitetsnivå sannolik och osäker krävs alltså att den person som ska registreras faktiskt inställer sig personligen hos en myndighet som kan ta upp biometriska underlag. Det innebär antingen att den myndighet som efterfrågar registrering i ett index behöver ta upp det biometriska underlag som ska ligga till grund för registrering i indexet eller att personen som ska registreras inställer sig personligen hos en annan myndighet. Vi ser problem med båda dessa lösningar.

Som vi återkommer till i avsnitt 13.4 bör Skatteverket, Migrationsverket och Polismyndigheten – som redan i dag har en central roll för den statliga identitetsförvaltningen – ansvara för registrering av en identitetsnyckel i ett nationellt identitetsindex. En sammanhållen identitetsförvaltning bör eftersträvas, vilket också framgår av våra direktiv. Det är enligt vår mening inte lämpligt att låta andra myndigheter ta upp biometriska underlag som ligger till grund för registrering i ett index. Många aktörer kan medföra utmaningar med samordning, för att till exempel säkerställa enhetliga rutiner för upptagning av biometriska underlag. Vidare har andra myndigheter i dag varken rättsliga eller praktiska möjligheter att ta upp biometriska underlag och därmed inte sådan kompetens och erfarenhet som vi bedömer är nödvändig för att säkerställa hög kvalitet på underlagen och i förlängningen de biometriska underlag och uppgifter som registreras i indexet.

Under förutsättning att en person som uppmanas av till exempel Försäkringskassan att inställa sig personligen hos Skatteverket, Migrationsverket eller Polismyndigheten för att lämna biometriska underlag följer uppmaningen kan han eller hon registreras i ett identitetsindex. Det är dock rimligt att anta att det kommer att finnas personer som

[6] *Stärkt system för samordningsnummer,* prop. 2021/22:276, s. 59 f.

– av olika anledningar – inte inställer sig för upptagning av biometriska underlag efter en sådan uppmaning. Utan möjlighet att ta till åtgärder för att få en person att inställa sig riskerar uppmaningen att bli verkningslös, och om personen blir registrerad i indexet eller inte beror därmed på dennes vilja och möjligheter att inställa sig. Det är enligt vår bedömning inte lämpligt att den enskilde kan föreläggas att inställa sig, med eller utan vite, eller att den enskilde ska kunna hämtas och fysiskt tvingas lämna biometriskt underlag. Vidare är det, enligt vår bedömning, inte heller rimligt att fortsatt handläggning av ärendet hos den myndighet som efterfrågat registrering i ett index villkoras av att personen i fråga faktiskt inställer sig för upptagning av biometriska underlag och blir registrerad i ett index. Det bör till exempel inte vara en förutsättning att den enskilde blir registrerad för att han eller hon ska kunna beviljas en förmån eller ett tillstånd av något slag. Vidare kan det bli problematiskt till exempel för en bilägare om Transportstyrelsen inte skulle kunna registrera ett ägarbyte i vägtrafikregistret, om den nya ägarens identitet inte går att verifiera genom kontroll mot ett identitetsindex.[7]

De omständigheter vi redogjort för ovan leder oss till slutsatsen att registrering av en person i ett identitetsindex inte bör kunna initieras av andra aktörer än Skatteverket, Migrationsverket och Polismyndigheten. Ett undantag är emellertid ärenden där det i ett beslut om en kvalificerad skyddsidentitet förordnas att en identitetsnyckel ska skapas. Vi återkommer till detta i avsnitt 13.3.8.

13.2.7 Rättsligt stöd för att ta upp och behandla biometriska underlag och uppgifter

Vår bedömning

Det finns ett rättsligt stöd för att ta upp biometriska underlag i de situationer då en identitetsnyckel, enligt våra bedömningar, bör kunna skapas.

Det behövs kompletterande bestämmelser i nationell rätt för att säkerställa att ovanstående myndigheters behandling av de bio-

[7] Jfr med situationen att ett ägarbyte inte skulle kunna registreras i vägtrafikregistret med anledning av att köparen endast har ett samordningsnummer på identitetsnivå sannolik eller osäker, Utredningsuppdrag, Uppdrag att säkerställa att information från folkbokföringen och information om samordningsnummer används ändamålsenligt, dnr TSG 2024-5982, 2025-05-09, s. 19.

metriska underlagen och de biometriska uppgifter som tas fram ur dessa – för syftet identitetsindex – är förenlig med det EU-rättsliga dataskyddsregelverket.

Utan rättsligt stöd för att ta upp biometriska underlag från en person är det inte möjligt att skapa en unik identitetsnyckel i ett identitetsindex. Befintliga regelverk ger redan i dag Migrationsverket – inklusive utlandsmyndigheterna – Polismyndigheten och Skatteverket rättsligt stöd för att under vissa förutsättningar ta upp biometriska underlag i respektive myndighets verksamhet. Det finns också förslag om utökad användning av biometriska uppgifter i dessa myndigheters verksamhet, vilket vi redogjort för i kapitel 7. Våra bedömningar i detta kapitel utgår från såväl befintligt och beslutat som föreslaget rättsligt stöd för att ta upp biometriska underlag. Även Regeringskansliet – i form av Utrikesdepartementet – kan ta upp biometriska underlag, vid handläggning av ärenden om uppehållstillstånd för diplomater.[8] Eftersom vi bedömer att diplomater bör undantas från registrering i ett identitetsindex (se avsnitt 12.4.6) berörs Regeringskansliets möjligheter i dessa avseenden dock inte.

Som framgår ovan anser vi att registrering i ett identitetsindex som utgångspunkt bör kunna göras endast när en myndighet faktiskt tar upp biometriska underlag av annan anledning än registrering i indexet, det vill säga i samband med handläggningen av ett visst ärende. Det kommer därmed att finnas ett rättsligt stöd för berörda myndigheter att ta upp biometriska underlag i aktuella situationer.

Vid införande av ett system med ett identitetsindex, och registrering i indexet i de situationer vi i det här kapitlet bedömer är lämpliga, kommer de biometriska underlagen dock att användas även för andra ändamål än de som de primärt tas upp för. Migrationsverkets – inklusive utlandsmyndigheternas – och Polismyndighetens möjligheter att ta upp biometriska underlag i enlighet med regelverket i 9 kap. utlänningslagen (2005:716) har andra syften än att möjliggöra framtida verifiering genom kontroll mot ett identitetsindex. Vidare får uppgifter om fingeravtryck och fotografier i Migrationsverkets register användas endast för de ändamål som specificeras i 15 § utlänningsdatalagen (2016:27). Dessa ändamål innefattar varken

[8] Jfr 9 kap. 8 a § utlänningslagen (2005:716), 4 kap. 19 § utlänningsförordningen (2006:97) och *Återkallelse av uppehållstillstånd som har meddelats av Regeringskansliet för personer med anknytning till utländska beskickningar, karriärkonsulat eller internationella organ*, prop. 2021/22:121, s. 7.

registrering i ett identitetsindex eller efterföljande användning av uppgifterna i ett sådant system. Den efterföljande behandlingen i ett identitetsindex av biometriska underlag som berörda myndigheter tar upp – och av de biometriska uppgifter som tas fram ur dessa – behöver enligt vår bedömning regleras i nationell rätt. Detta för att ge myndigheterna förutsättningar att behandla personuppgifter – inklusive biometriska uppgifter – på ett ändamålsenligt sätt och för att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Som framgår av tabell 10.1 i avsnitt 10.3.2 finns det förhållandevis begränsade befintliga och föreslagna möjligheter att lagra biometriska underlag och de biometriska uppgifter som kan tas fram ur dessa i befintliga register som förs av Polismyndigheten, Migrationsverket och Skatteverket.

13.2.8 Personkategorier som bör undantas

Vår bedömning

Barn som inte har fyllt sex år samt diplomatisk personal bör undantas från registrering i ett identitetsindex.

Det saknas, enligt vår tidigare bedömning, behov av att barn som inte har fyllt sex år och diplomatisk personal omfattas av ett identitetsindex (se avsnitt 12.4.1 och 12.4.6). Utifrån de bedömningar vi gör nedan – om i vilka situationer en identitetsnyckel bör skapas – kan personer i dessa kategorier emellertid komma att träffas av ett regelverk för registrering. Som exempel kan nämnas att Polismyndigheten tar upp biometriska underlag i form av ansiktsbild för barn som inte har fyllt sex år vid ansökan om pass (se avsnitt 13.3.2). För diplomatisk personal kan biometriska underlag komma att tas upp vid utfärdande av uppehållstillståndkort (se avsnitt 13.3.5). Diplomatisk personal är enligt 2 kap. 10 § utlänningslagen undantagen krav på pass, visering, uppehållstillstånd och arbetstillstånd. Trots detta beviljas, utöver viseringar när sådana behövs, uppehållstillstånd för personer med anknytning till utländska beskickningar

och karriärkonsulat. Att uppehållstillstånd beviljas medför praktiska fördelar, exempelvis i samband med resor.[9]

För att säkerställa att barn som inte har fyllt sex år samt diplomatisk personal inte registreras i ett identitetsindex bör de uttryckligen undantas från registrering.

13.3 Ärenden i vilka en identitetsnyckel bör skapas

Med ovan redovisade utgångspunkter behöver det närmare belysas i vilka ärendeslag som en identitetsnyckel bör kunna skapas. Tänkbara ärendeslag är bland annat de där en svensk rese- eller identitetshandling utfärdas. Vi har i våra fortsatta överväganden i dessa delar – i enlighet med våra direktiv – utgått från de förslag som lämnats i promemorian *Ett statligt identitetskort* (Ju2026/01595) om att ett statligt identitetskort ska ersätta dels identitetskort för folkbokförda, dels nationella identitetskort. Vidare har förslag lämnats i promemorian *Avveckling av Skatteverkets id-kortsverksamhet* (Fi2026/01416) om att denna verksamhet ska avvecklas. Vi utvärderar därför inte om en identitetsnyckel bör kunna skapas vid utfärdande av identitetskort för folkbokförda och nationella identitetskort. Vi har vidare utgått från de förslag som lämnats i propositionen *En statlig e-legitimation*, prop. 2025/26:250.

13.3.1 Medborgarskapsärenden

Vår bedömning

En identitetsnyckel bör kunna skapas i samband med att biometriska underlag tas upp vid en anmälan eller ansökan om svenskt medborgarskap.

Förvärv av svenskt medborgarskap genom anmälan eller ansökan regleras i 6–12 §§ medborgarskapslagen. Förutom vid förvärv enligt bestämmelsen i 10 § för barn till föräldrar som får svenskt medborgarskap med stöd av bestämmelserna i 6–9 §§, är ett gemensamt krav

[9] *Återkallelse av uppehållstillstånd som har meddelats av Regeringskansliet för personer med anknytning till utländska beskickningar, karriärkonsulat eller internationella organ*, prop. 2021/22:121, s. 7 f.

att utlänningen ska ha permanent uppehållstillstånd. Det ligger i sakens natur att svenskt medborgarskap, som utgångspunkt, inte kan förvärvas av den som endast har ett tidsbegränsat uppehållstillstånd; vissa undantag för personer som har välgrundade utsikter att beviljas varaktigt uppehållstillstånd finns dock i 20 §. Med permanent uppehållstillstånd likställs, enligt 20 §, uppehållsrätt enligt rörlighetsdirektivet[10]. Brittiska medborgare som har beviljats uppehållsstatus undantas också från kravet på permanent uppehållstillstånd. För samtliga uppställs emellertid ett krav på att ha haft hemvist i landet under en viss tid för att kunna förvärva svenskt medborgarskap. Kravet ger framför allt uttryck för tanken att en person ska känna till svenska förhållanden och vara en del av det svenska samhället. Individen anses då ha en sådan samhörighet med Sverige att han eller hon som huvudregel ska kunna blir svensk medborgare.[11] För förvärv av svenskt medborgarskap efter ansökan (naturalisation) krävs enligt huvudregeln åtta års hemvist i Sverige. För barn mellan 15 och 18 år krävs mellan tre och fem års hemvist och för självständig naturalisation av barn under 15 år ställs normalt inget krav på viss hemvisttid, förutsatt att någon av föräldrarna är svensk medborgare.[12]

Även om det finns vissa möjligheter till undantag från både kravet på permanent uppehållstillstånd och hemvist i Sverige kan det enligt vår bedömning med fog antas att den absoluta merparten av de som förvärvar medborgarskap genom en anmälan eller ansökan har haft kontakt med Migrationsverket tidigare i ett ärende om uppehållstillstånd, eller med Skatteverket i ett ärende inom folkbokföringsverksamheten. Enligt vår bedömning i avsnitt 13.3.5–13.3.7 bör en identitetsnyckel skapas vid utfärdande av uppehållstillståndskort – efter beviljande av uppehållstillstånd – samt i vissa ärenden om folkbokföring och samordningsnummer. En identitetsnyckel kommer därför normalt sett inte behöva skapas vid förvärv av svenskt medborgarskap genom anmälan eller ansökan. Oaktat detta är det viktigt att fånga upp personer som vill bli svenska medborgare och inte tidigare är registrerade i ett identitetsindex.

Att biometriska underlag kan tas upp är en förutsättning för att en identitetsnyckel ska kunna skapas. Medborgarskapslagen innehåller i nu gällande lydelse inte någon bestämmelse om upptagning

[10] Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004.
[11] *Ett medborgarskap som grundas på samhörighet,* prop. 2013/14:143, s. 12 f.
[12] Jfr MIG 2021:12, *Lag om svenskt medborgarskap,* prop. 1999/2000:147, s. 33 och *Skärpta krav för svenskt medborgarskap,* prop. 2025/26:175, s. 131 ff.

av biometriska underlag. Vi har dock i vårt arbete att utgå från de förslag som lämnats i propositionen *Stärkt återvändandeverksamhet*, bland annat om att en ny bestämmelse ska införas i 13 f § medborgarskapslagen. Enligt förslaget ska den myndighet som ska pröva ansökan eller anmälan få fotografera en utlänning som har uppehållstillstånd och, om han eller hon har fyllt sex år, ta hans eller hennes fingeravtryck. Den föreslagna bestämmelsen skulle enligt vår mening ge ett tillräckligt stöd för Migrationsverket att ta upp de biometriska underlag som skulle kunna lagras i ett identitetsindex. Bestämmelsen är visserligen fakultativt utformad och en bedömning av om det är proportionerligt och nödvändigt att ta upp fingeravtryck får, enligt författningskommentaren till den föreslagna bestämmelsen, göras i det enskilda fallet. Som exempel på en situation där det skulle kunna vara oproportionerligt att ta upp fingeravtryck nämns ärenden som rör barn och där det saknas tvivel om barnets identitet.[13] Som vi pekat på ovan kan det antas att merparten av personer som förekommer i dessa ärenden tidigare kommer att ha haft kontakt med Migrationsverket eller Skatteverket och då kunnat registrerats i ett index; syftet med den identitetskontroll som möjliggörs genom den föreslagna bestämmelsen är att kontrollera att den som förekommer i medborgarskapsärendet också är den person som har beviljats uppehållstillstånd i Sverige.[14] Det kan därför antas att det i praktiken skulle vara relativt få av de personer som vill bli svenska medborgare som inte kan fångas upp i ett index, på grund av att den föreslagna bestämmelsen i 13 f § medborgarskapslagen är fakultativt utformad.

Frågan är när under handläggningen av en ansökan eller anmälan om svenskt medborgarskap som en identitetsnyckel bör skapas. Ett alternativ är att knyta tidpunkten till när anmälan eller ansökan ges in. Det kan emellertid tänkas att en ansökan avskrivs, exempelvis för att utlänningen inte betalar in ansökningsavgiften eller återtar sin ansökan eller anmälan. Detta talar i viss mån mot att en identitetsnyckel skapas i ett så tidigt skede. Det är inte heller säkert att biometriska underlag tas upp vid den tidpunkten.

Ett annat alternativ skulle kunna vara att knyta skapandet av en nyckel till beslutstidpunkten. Detta är enligt vår bedömning dock inte möjligt. Enligt förslaget till ny bestämmelse i 13 f § medborgar-

[13] Prop. 2025/26:263, s. 8, 129 ff. och 155 ff. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.
[14] Prop. 2025/26:263, s. 130 f.

skapslagen ska det biometriska underlag som tagits upp i samband med kontrollen *omedelbart* förstöras om kontrollen visar att uppgifterna motsvarar de uppgifter som finns sparade i uppehållstillståndskortet eller i de register som förs enligt 15 § utlänningsdatalagen. I många fall skulle det därför kunna vara så att det vid den tidpunkt då ett beslut fattas i ärendet inte längre finns några biometriska underlag som kan lagras i ett identitetsindex. Det finns enligt vår bedömning inte något som talar för att det endast skulle finnas behov av att i indexet registrera personer vars biometriska uppgifter *inte* stämmer med de som tidigare registrerats.

Mot bakgrund av det ovan anförda anser vi att det inte är lämpligt att en identitetsnyckel skapas vid ansöknings- eller anmälningstillfället, eller när beslut fattas i ärendet. En identitetsnyckel bör i stället skapas när de biometriska underlagen tas upp vid en anmälan eller ansökan om svenskt medborgarskap. Vid denna tidpunkt är utgången i ärendet om svenskt medborgarskap dock inte bestämd. Med utgångspunkt i vår bedömning kan det därmed vara så i det enskilda fallet att en identitetsnyckel kommer att skapas även för den som inte förvärvar svenskt medborgarskap. Med hänsyn till att det, som utgångspunkt, är fråga om personer som har en mycket tydlig anknytning till Sverige och i normalfallet har varit bosatta i landet under en längre tid, samt som – genom anmälan eller ansökan – har manifesterat en vilja att fortsatt ha sin hemvist i landet och att ta del av de rättigheter och skyldigheter som följer med medborgarskapet, anser vi emellertid att det finns ett tydligt behov av att registrera även de som får avslag på sin ansökan eller anmälan. Bifallsandelen i dessa ärendeslag är vidare relativt hög, vilket – i kombination med det ovan anförda – talar för att endast ett mindre antal individer kommer att registreras trots att de inte förvärvar svenskt medborgarskap; av statistik från Migrationsverket framgår följande angående antalet inkomna och avgjorda ärenden under år 2022–2025.[15]

[15] https://www.migrationsverket.se/om-migrationsverket/statistik/svenskt-medborgarskap.html, senast besökt den 3 juli 2026.

Tabell 13.1 Inkomna och avgjorda ärenden om svenskt medborgarskap

År	2022	2023	2024	2025
Anmälan				
– inkomna	19 925	15 544	14 438	15 212
– avgjorda	17 934	15 532	16 635	13 918
– bifall	14 373	12 357	12 945	10 851
– avslag	2 492 (20 %)	2 158 (20 %)	2 624 (22 %)	2 084 (22 %)
Ansökan				
– inkomna	65 990	57 662	49 701	41 000
– avgjorda	74 086	58 541	55 725	34 881
– bifall	62 393	46 741	43 758	21 830
– avslag	10 641 (16 %)	10 958 (20 %)	11 034 (21 %)	12 015 (37 %)

Sammantaget anser vi alltså att en identitetsnyckel bör skapas när biometriska underlag tas upp i samband med en anmälan eller ansökan om svenskt medborgarskap.

13.3.2 Utfärdande av pass

Vår bedömning

En identitetsnyckel bör kunna skapas när ett pass utfärdas, dock inte om det utfärdas av en utlandsmyndighet.

Vid ansökan om ett pass ska en noggrann identitetskontroll göras av den utfärdande myndigheten, som inom riket är Polismyndigheten. Sökanden är enligt 6 § passlagen (1978:302) skyldig att inställa sig personligen och ska då styrka sin identitet, sitt svenska medborgarskap och övriga personuppgifter. Identitetskontrollen och kravet på styrkt identitet främjar att korrekta uppgifter kan registreras i ett identitetsindex i dessa ärenden. För att en svensk medborgare ska kunna få ett pass utfärdat måste han eller hon ha ett personnummer alternativt ett samordningsnummer; en identitetsbeteckning kommer därmed att kunna registreras i indexet vid registrering i samband med utfärdande av pass.

Det finns ett rättsligt stöd för att ta upp biometriska underlag i form av både ansiktsbild och fingeravtryck vid ansökan, enligt 6 § passlagen. De biometriska uppgifterna får, enligt gällande bestäm-

melser, inte sparas i passregistret. För det fall en identitetsnyckel ska kunna skapas i samband med ett ärende om pass kommer de biometriska uppgifter som tagits fram ur underlaget som tagits upp i dessa ärenden däremot att behöva lagras i identitetsindexet. Vi anser dock att nuvarande begräsningar avseende lagring av biometriska uppgifter inte utgör ett hinder mot att skapa en identitetsnyckel i samband med en ansökan om pass. Att inte på ett effektivt sätt kunna fånga upp en majoritet av dem som vi anser bör omfattas av ett identitetsindex skulle som vi ser det direkt motverka syftet och nyttan med det. Vi kan vidare konstatera att det i promemorian *Ett statligt identitetskort* har lämnats förslag om införande av ett pass- och identitetskortsregister som ska få innehålla biometriska uppgifter som har tagits fram ur den ansiktsbild som tas av sökanden.[16] Steg har alltså redan tagits som möjliggör att biometriska uppgifter får lagras och användas för andra ändamål än vad som i nuläget är möjligt.

Ett pass är giltigt under en begränsad tid; ett svenskt pass har en giltighetstid på fem år för vuxna och tre år för barn under 12 år. Handlingen behöver alltså förnyas med viss regelbundenhet. Att detta också sker i praktiken får stöd av statistiken.[17]

Tabell 13.2 Utfärdade pass år 2023–2025

År	2023	2024	2025
Pass (inkl. extra pass)	1 591 928	1 686 245	1 448 159

Ett relativt stort antal pass utfärdas alltså varje år, vilket enligt vår bedömning kan möjliggöra att en stor mängd personer kan fångas upp relativt snabbt. En potentiell nackdel är att många registreringar därmed kan behöva göras åtminstone i ett inledande skede efter att ett identitetsindex har tagits i drift. Antalet ärenden kan enligt vår bedömning dock inte antas bli så många att det skulle medföra en orimlig eller omöjlig arbetsbörda för Polismyndigheten. Detta särskilt med hänsyn till att åtgärderna i stora delar kan vidtas inom ramen för de handläggningsåtgärder som redan vidtas i ärenden om pass.

Frågan är vid vilken tidpunkt en identitetsnyckel bör skapas i ett ärende om pass. De biometriska underlag som tagits upp vid en ansökan kommer att vara tillgängliga vid den tidpunkt då passet utfärdas

[16] Ju2026/01595, s. 129 ff.
[17] Polismyndighetens årsredovisning för år 2025, s. 100.

och därefter lämnas ut till sökanden, om ansökan inte återkallats eller avslagits. Detta framgår av 6 a § passlagen. Det är därmed inte, på samma sätt som vid en ansökan eller anmälan om svenskt medborgarskap, nödvändigt att knyta skapandet av en identitetsnyckel till tidpunkten för när de biometriska underlagen tas upp i ärendet. Att en nyckel skapas redan innan handlingen utfärdas kan visserligen antas stärka den kontroll som sker i samband med utlämnandet. Om den skapas redan i samband med att de biometriska underlagen tas upp finns däremot risk för att även personer som får avslag på en ansökan, exempelvis för att sökanden inte har styrkt sin identitet på föreskrivet sätt (se 7 § passlagen), registreras i indexet. Detta bör enligt vår mening undvikas i den mån det är möjligt för att främja att så korrekta uppgifter som möjligt registreras, och kan effektivt förhindras genom att skapandet av en identitetsnyckel knyts till utfärdandetidpunkten. Vid den tidpunkten kan utredningen i ärendet också antas vara fullständig. Vi anser att det i övrigt inte har kommit fram omständigheter som talar mot en sådan ordning. En identitetsnyckel bör alltså skapas när ett pass utfärdas. Som vi återkommer till i avsnitt 13.4.2 bör en identitetsnyckel däremot inte skapas om passet utfärdas av en utlandsmyndighet.

En fråga i detta sammanhang är om EU:s passförordning[18] innebär hinder mot att lagra den ansiktsbild som tagits vid ansökan om ett pass och de biometriska uppgifter som kan tas fram ur denna. Förordningen innehåller standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar och syftar till att skapa mer harmoniserade säkerhetsstandarder för pass och resehandlingar som skydd mot förfalskning. Genom förordningen harmoniseras säkerhetsdetaljer och införande av biometriska kännetecken, vilket är ett viktigt steg på vägen för att göra resehandlingar säkrare och skapa en mer tillförlitlig koppling mellan innehavaren och passet eller resehandlingen och därigenom bidra till att förhindra att de används i bedrägligt syfte (skäl 3). Enligt förordningen ska pass och resehandlingar innehålla ett lagringsmedium, som i sin tur ska innehålla en ansiktsbild och två fingeravtryck (artikel 1.2). Förordningen är tillämplig på pass och resehandlingar som utfärdas av medlemsstaterna. Den är inte tillämplig på identitetskort som medlemsstaterna utfärdar till sina medborgare (artikel 1.3).

[18] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004.

Vid tillämpning av förordningen får de biometriska kännetecknen i pass och resehandlingar endast användas för att kontrollera antingen passets eller resehandlingens autenticitet eller innehavarens identitet, genom direkt tillgängliga jämförbara kännetecken, när uppvisande av pass eller resehandling krävs enligt lag (artikel 4.3). Förordningen innehåller emellertid inte några bestämmelser som hindrar att de biometriska underlagen som tagits upp får lagras även på annat sätt än i lagringsmediet på det pass eller den resehandling som utfärdas med stöd av förordningen; ansiktsbilden lagras redan i dag i passregistret, och i det förslag till ny pass- och identitetskortsdatalag som lämnats i promemorian *Ett statligt identitetskort* framgår att såväl ansiktsbilder som tagits vid en passansökan som de biometriska uppgifter som tagits fram ur ansiktsbilderna ska få lagras i ett pass- och identitetskortsregister.[19] I promemorian föreslogs vidare att det i samband med ansökan om pass – och statligt identitetskort – ska vara möjligt för den utfärdande myndigheten att göra sökningar på ansiktsbilder och biometriska uppgifter i pass- och identitetskortsregistret.[20] Dessa uppgifter kommer därmed att användas för delvis andra syften än de som de tagits upp för.

Vi bedömer mot denna bakgrund att förordningen inte utgör hinder för att lagra motsvarande underlag och uppgifter även i ett identitetsindex och använda dem för andra syften, så länge lagringen och användningen är förenlig med grundläggande rättigheter och dataskyddsförordningen.

13.3.3 Utfärdande av ett statligt identitetskort

Vår bedömning

En identitetsnyckel bör kunna skapas när ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort* (Ju2026/01595) utfärdas, dock inte om kortet utfärdas av en utlandsmyndighet.

I promemorian *Ett statligt identitetskort* föreslogs bland annat att ett statligt identitetskort ska kunna utfärdas till svenska medborgare,

[19] Ju2026/01595, s. 130 ff. och 139 ff.
[20] Ju2026/01595, s. 139.

till utlänningar som är folkbokförda i Sverige, till utlänningar som har tilldelats ett personnummer enligt 18 b § folkbokföringslagen (1991:481) och som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall samt till utlänningar som, efter att ha styrkt sin identitet, har tilldelats ett samordningsnummer enligt lagen (2022:1697) om samordningsnummer, under förutsättning att numret inte är förklarat vilande. Det statliga identitetskortet ska för utlänningar utfärdas utan funktion som resehandling. Det är tänkt att ersätta det nationella identitetskortet för svenska medborgare respektive det identitetskort för personer som är folkbokförda i Sverige som Polismyndigheten respektive Skatteverket i nuläget utfärdar. Skatteverkets id-kortsverksamhet ska enligt förslag i promemorian *Avveckling av Skatteverkets id-kortsverksamhet* (Fi2026/01416) avvecklas. Det föreslagna statliga identitetskortet ska utfärdas av Polismyndigheten, i likhet med vad som gäller för pass och nationella identitetskort i dag.[21]

Enligt förslagen i promemorian *Ett statligt identitetskort* ska ansökningsprocessen i allt väsentligt fungera på samma sätt som vid en ansökan om pass och nationella identitetskort.[22] Sökanden ska som utgångspunkt inställa sig personligen och är skyldig att styrka sin identitet och övriga personuppgifter som krävs för att identitetskortet ska kunna utfärdas. Vid en ansökan om ett identitetskort med funktion som resehandling ska sökanden dessutom styrka sitt svenska medborgarskap. Biometriska underlag i form av ansiktsbild och fingeravtryck ska – på samma sätt som vid ansökan om pass – tas upp i samband med ansökan och det pass- och identitetskortsregister som föreslagits ska få innehålla biometriska uppgifter som har tagits fram ur den ansiktsbild som tas av sökanden.[23]

Det föreslagna statliga identitetskortet ska normalt sett vara giltigt under fem år, och kommer alltså att behöva förnyas med viss regelbundenhet. Eftersom det är tänkt att ersätta nationella identitetskort kan det antas att ungefär lika många ärenden aktualiseras per år som för dessa handlingar, se nedanstående tabell avseende statistik från Polismyndigheten.[24]

[21] Ju2026/01595, s. 59 och 63.
[22] Ju2026/01595, s. 70 f. och 75 f.
[23] Ju2026/01595, s. 76 och 139.
[24] Polismyndighetens årsredovisning 2025, s. 100.

Tabell 13.3 Utfärdade nationella identitetskort 2023–2025

År	2023	2024	2025
Nationella identitetskort	527 665	601 180	514 162

Beträffande det identitetskort för personer som är folkbokförda i Sverige som Skatteverket utfärdar framgår att myndigheten under år 2017 handlade cirka 160 000 ansökningar om sådana kort.[25] Även om det är svårt att dra några slutsatser avseende de förslag om ett nytt statligt identitetskort som lämnats bedömer vi – utifrån den förslagna giltighetstiden och antalet ärenden om nationella identitetskort och det identitetskort för personer som är folkbokförda i Sverige som Skatteverket handlägger – att förhållandevis många personer, såväl svenska medborgare som utländska medborgare som är bosatta i Sverige, kan komma att fångas upp på detta sätt. Att identitetskortet ska kunna innehålla en statlig e-legitimation[26] – vilket ökar användbarheten för enskilda – talar enligt vår mening i samma riktning. Syftet med ett identitetsindex skulle därmed främjas väsentligt om en identitetsnyckel kan skapas vid en ansökan om ett sådant statligt identitetskort som har föreslagits. Detta inte minst genom att det är möjligt att fånga upp personer som, vid tidpunkten då ett index kan komma att tas i drift, vistas i Sverige och inte på andra sätt som beskrivs i detta kapitel kan registreras i indexet, exempelvis vid en anmälan om inflyttning.

Sammantaget anser vi därför att det är ändamålsenligt att en identitetsnyckel skapas inom ramen för ett ärende om ett statligt identitetskort. En nyckel bör – på de skäl som anförts avseende pass – skapas vid utfärdandetidpunkten. Som vi återkommer till i avsnitt 13.4.2 bör en nyckel dock inte skapas om handlingen utfärdas av en utlandsmyndighet.

I likhet med vad som gäller för pass finns det på EU-nivå en reglering av utformningen av identitetskort för unionsmedborgare. Den förordning om säkrare identitetskort som antogs i juni 2019[27] skärpte säkerhetskraven på nationella identitetskort. I dom i målet C-61/22, *Landeshaupstadt Wiesbaden*, kom EU-domstolen dock fram till att förordningen var ogiltig. Anledningen var att lagstiftaren inte tillämpat

[25] *Ett säkert statligt ID-kort – med e-legitimation*, SOU 2019:14, s. 216 och 375.
[26] Ju2026/01595, s. 92 f.
[27] Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019.

ett korrekt lagstiftningsförfarande. Med anledning av det antogs den nu gällande id-kortsförordningen[28] i juni 2025. Frågan är om förordningen utgör hinder mot att den ansiktsbild som tas upp i samband med ansökan av det föreslagna statliga identitetskortet – och de biometriska uppgifter som kan tas fram ur ansiktsbilden – lagras i ett identitetsindex.

I skäl 20 i den nya id-kortsförordningen anges att förordningen inte utgör rättslig grund för att upprätta eller underhålla databaser på nationell nivå för lagring av biometriska uppgifter i medlemsstaterna, vilket är en fråga för nationell rätt som måste vara förenlig med unionens dataskyddslagstiftning, inbegripet nödvändighets- och proportionalitetskraven. Artikel 10 i förordningen reglerar insamling av de biometriska kännetecken som enligt förordningen ska lagras på identitetskorten. Biometriska kännetecken som lagras för personalisering av identitetskort ska förvaras på ett mycket säkert sätt och aldrig längre än 90 dagar från den dag då handlingen utfärdats. Efter denna period ska de biometriska kännetecknen omedelbart raderas eller förstöras. Av sista meningen i artikel 10.3 – som är ett tillägg i förhållande till dels den tidigare gällande id-kortsförordningen 2019/1157[29], dels till förslaget till nu gällande förordning – framgår emellertid att detta inte ska påverka lagring av dem när detta krävs enligt unionsrätten eller nationell rätt, i enlighet med unionens dataskyddslagstiftning.

Europeiska datatillsynsmannen (EDPS) – som är en tillsynsmyndighet för EU:s institutioner, organ och byråer och har till uppgift att säkerställa att personuppgifter behandlas på ett lagligt och korrekt sätt inom EU – lämnade vissa synpunkter på förslaget till gällande id-kortsförordning. EDPS uttryckte bland annat oro över att den föreslagna förordningen inte uteslöt den rättsliga möjligheten att ha databaser för lagring av biometriska uppgifter på nationell nivå enligt nationell rätt. EDPS betonade att sådana databaser på nationell nivå, tillsammans med den potentiella användningen av biometriska uppgifter för andra ändamål, skulle behöva uppfylla ett strikt nödvändighets- och proportionalitetstest enligt stadgan, så som den tolkas enligt EU-domstolen. Vidare påpekade EDPS att databaser med biometriska uppgifter inte bara riskerar att användas felaktigt eller till och med missbrukas, utan också kan vara väldigt sårbara vid data-

[28] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.
[29] Jfr EU-domstolens uttalande om artikel 10.3 i förordning 2019/1157 i mål C-61/22 (punkt 113).

intrång, till exempel på grund av en cyberattack. I sitt yttrande rekommenderade därför EDPS att förslagets formuleringar stärktes så att möjligheten att inrätta eller underhålla databaser för lagring av biometriska uppgifter som samlats in enligt nuvarande förordning och förslaget utesluts helt eller begränsas väsentligt.[30] Vi kan emellertid notera att lydelsen av skäl 19 i förslaget till id-kortsförordningen, som bland annat kritiserades av EDPS, inte ändrades i samband med att förordningen antogs (skäl 19 motsvarar skäl 20 i den antagna förordningen). Dessutom talar – som vi ser det – tillägget i sista meningen i artikel 10.3 i id-kortsförordningen uttryckligen för att biometriska underlag som tas upp i samband med en ansökan om identitetskort får användas även för andra syften, så länge användningen är förenlig med grundläggande rättigheter och med dataskyddsförordningen.

Mot den här bakgrunden bedömer vi att id-kortsförordningen inte utgör hinder mot att skapa en identitetsnyckel i samband med en ansökan om ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort*.

13.3.4 Utfärdande av en statlig e-legitimation

Vår bedömning

En identitetsnyckel bör kunna skapas när en sådan statlig e-legitimation som har föreslagits i propositionen *En statlig e-legitimation* utfärdas.

I betänkandet *En säker och tillgänglig statlig e-legitimation* föreslogs bland annat att en statlig e-legitimation på tillitsnivå hög ska införas.[31] Enligt förslag i den efterföljande propositionen *En statlig e-legitimation* ska den statliga e-legitimationen tillhandahållas efter ansökan till den som vid personlig inställelse har styrkt sin identitet och är svensk medborgare, utländsk medborgare och folkbokförd eller har ett så kallat immunitetsnummer och omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall. Polismyndigheten ska vara utfärdande myndighet inom riket. För att få en statlig e-legitimation ska det, enligt propositionen, krävas att sökanden har fyllt eller inne-

[30] Se förslag (COM[2024] 316 final) och Opinion 21/2024 on Proposal for a Council Regulation on strengthening the security of identity cards, den 13 september 2024.
[31] SOU 2023:61.

varande kalenderår ska fylla nio år. Giltighetstiden ska enligt förslagen begränsas till fem år. Om sökanden inte har fyllt tolv år ska giltighetstiden vara tre år.[32] I samband med ansökan ska sökanden – enligt 2 kap. 4 § i förslag till lag om statlig e-legitimation och elektronisk identifiering – vara skyldig att låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck. Ansiktsbilden som tas i samband med ansökan ska enligt 2 kap. 5 § i förslaget till ny lag sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Om fingeravtryck har tagits ska även dessa sparas i lagringsmediet.

Det saknas av naturliga skäl statistik kring antalet ärenden om en statlig e-legitimation. Vi kan även konstatera att enligt promemorian *Ett statligt identitetskort* ska det föreslagna statliga identitetskortet kunna vara bärare av en statlig e-legitimation[33]. Vidare föreslås att den föreslagna lagen om statlig e-legitimation och elektronisk identifiering ska upphävas i samband med att det statliga identitetskortet införs. Med hänsyn till detta kan antalet ärenden om utfärdande av en statlig e-legitimation med stöd av lagen om statlig e-legitimation och elektronisk identifiering i praktiken förväntas bli relativt begränsade, och endast förekomma under en övergångsperiod. Oaktat detta anser vi att det kan vara av vikt att ha möjlighet att fånga upp den personkrets som ska kunna få en statlig e-legitimation utfärdad även inom ramen för ett sådant ärende. Sammantaget anser vi därför att en identitetsnyckel bör kunna skapas i ett ärende om en sådan statlig e-legitimation som har föreslagits i propositionen *En statlig e-legitimation*. En nyckel bör enligt vår mening – på de skäl som anförts avseende pass – i så fall skapas vid utfärdandetidpunkten.

13.3.5 Utfärdande av uppehållstillståndskort

Vår bedömning

En identitetsnyckel bör kunna skapas när ett uppehållstillståndskort med en giltighetstid om minst ett år utfärdas.

Enligt 4 kap. 22 § utlänningsförordningen (2006:97) ska ett bevis om uppehållstillstånd utfärdas i form av en sådan handling som avses i

[32] *En statlig e-legitimation*, prop. 2025/26:250, s. 23, 37 och 43.
[33] Ju2026/01595, s. 92.

EU-förordningen om uppehållstillståndskort[34]. En utlänning som ansöker om uppehållstillstånd är skyldig att låta Migrationsverket, en utlandsmyndighet eller Regeringskansliet fotografera honom eller henne och – om utlänningen har fyllt sex år – ta hans eller hennes fingeravtryck. Samma skyldighet gäller om ett uppehållstillståndskort ska utfärdas av annan anledning än att en utlänning ansöker om uppehållstillstånd. Det följer av 9 kap. 8 a § utlänningslagen. Åldersgränsen talar inte mot att en identitetsnyckel bör kunna skapas vid utfärdande av ett uppehållstillståndskort; i avsnitt 12.4.1 har vi bedömt att identitetsindexet endast bör omfatta personer som har fyllt sex år. I övrigt är möjligheten att ta upp biometriska underlag inte avhängig av några särskilda kriterier eller krav.

De biometriska underlagen är tillgängliga när uppehållstillståndskortet utfärdas; av 9 kap. 8 a § tredje stycket utlänningslagen framgår att ett fotografi och två fingeravtryck ska sparas i ett lagringsmedium i kortet. Fingeravtryck som inte sparas i ett sådant medium och de biometriska data som tas fram ur fingeravtrycken och ur fotografiet ska omedelbart förstöras när uppehållstillståndskortet har lämnats ut. Det finns inte något hinder enligt den ovan nämnda EU-förordningen eller den aktuella bestämmelsen i utlänningslagen mot att spara fotografiet i Migrationsverkets register.[35] Något hinder i förordningen mot att lagra fotografiet i ett identitetsindex kan enligt vår bedömning därför inte anses föreligga; förordningen innehåller inte någon bestämmelse om lagring av de biometriska underlagen som hindrar att de lagras även på annat sätt än i uppehållstillståndskortet, så länge användningen är förenlig med grundläggande rättigheter och med dataskyddsförordningen. Bestämmelsen i 15 § utlänningsdatalagen i dess nuvarande lydelse tillåter dock inte att fingeravtryck och fotografier som tas med stöd av 9 kap. 8 a § utlänningslagen sparas i Migrationsverkets register. I propositionen *Stärkt återvändandeverksamhet* har emellertid förslag lämnats om att biometriska underlag som tas upp med stöd av bestämmelsen ska få fortsatt behandlas i de register som Migrationsverket för och att regleringen om när fingeravtryck som tas med stöd av bestämmelsen ska förstöras ska upphävas.[36]

[34] Rådets förordning (EG) nr 1030/2002 av den 13 juni 2002 om en enhetlig utformning av uppehållstillstånd för medborgare i tredje land.
[35] *Biometriska kännetecken i uppehållstillståndskort*, prop. 2010/11:123 s. 25.
[36] Prop. 2025/26:263, s. 182.

Det skulle mot denna bakgrund vara möjligt att skapa en identitetsnyckel i samband med utfärdande av ett uppehållstillståndskort. Frågan är när under handläggningen som nyckeln bör skapas. Att en nyckel skapas redan i samband med att de biometriska underlagen tas upp skulle visserligen kunna antas stärka den kontroll som sker i samband med utlämnandet av kort. Samtidigt finns det då en risk för att även personer som får avslag på en ansökan registreras i ett identitetsindex. Detta kan effektivt förhindras genom att skapandet av en identitetsnyckel knyts till utfärdandetidpunkten. Vid den tidpunkten kan utredningen i ärendet också antas vara fullständig. Vidare står det då klart om personen ska beviljas ett uppehållstillstånd av sådan längd att han eller hon, enligt vår bedömning, bör registreras i ett identitetsindex. Ett sådant beslut och därmed utfärdandet av ett uppehållstillståndskort ska dessutom föregås av kontroller av om det finns hinder mot att bevilja uppehållstillstånd, exempelvis på grund av vandel eller att sökanden är upptagen på spärrlistan i Schengens informationssystem, SIS. Vi anser att det i övrigt inte kommit fram omständigheter som talar mot en sådan ordning.

Vi anser alltså att en identitetsnyckel bör skapas när ett uppehållstillståndskort utfärdas. På detta sätt kan flera kategorier av personer som har anknytning till Sverige men som inte på andra sätt som beskrivs i detta kapitel bör registreras i ett identitetsindex, komma att fångas upp, närmare bestämt de som, vid tidpunkten då ett index kan komma att tas i drift har ett uppehållstillstånd. Det är, enligt vår bedömning, dock endast personer som har beviljats ett uppehållstillstånd om minst ett år som bör omfattas av ett identitetsindex (jfr avsnitt 12.3.3). En nyckel bör därför skapas endast om giltighetstiden för uppehållstillståndskortet överstiger ett år.

13.3.6 Folkbokföringsärenden

Vår bedömning

En identitetsnyckel bör, om biometriska underlag har tagits upp vid en identitetskontroll, kunna skapas för den som folkbokförs efter flyttning till Sverige eller efter att ha varit avregistrerad som försvunnen, och för den som begär ändring av en uppgift om sin identitet.

Den som är folkbokförd i Sverige eller blir det genom inflyttning har, enligt vår bedömning (se avsnitt 12.3.1), en sådan anknytning till landet att han eller hon bör omfattas av ett identitetsindex. Vi kan konstatera att vid folkbokföring i samband med flyttning till Sverige kan det i många fall antas att en utlänning tidigare har haft kontakt med Migrationsverket i ett ärende om uppehållstillstånd, och därför har registrerats i ett identitetsindex vid utfärdande av ett uppehållstillståndskort. Det bör enligt vår mening emellertid, om möjligt, också finnas en självständig grund för att fånga upp personer som folkbokförs i landet, eftersom det finns personkategorier som inte behöver uppehållstillstånd i Sverige för att kunna folkbokföras här, exempelvis nordiska medborgare och EES-medborgare. Detta främjar att ett identitetsindex kan omfatta så många personer som möjligt i den personkrets som vi anser bör ingå.

En identitetsnyckel bör kunna skapas vid en identitetskontroll

En förutsättning för att en identitetsnyckel ska kunna skapas är att biometriska underlag kan ta upp i samband med detta. I folkbokföringsärenden finns ett sådant stöd i vissa särskilda situationer, som kan utläsas av bestämmelserna i 26–26 c §§ folkbokföringslagen. Vid en anmälan om flyttning från utlandet, och vid en anmälan av den som är avregistrerad som försvunnen och som ska folkbokföras, ska anmälaren inställa sig personligen hos Skatteverket. En identitetskontroll ska då genomföras enligt 26 a §. Enligt bestämmelsen i 26 b § ska den som innehar ett pass, ett identitetskort eller annan motsvarande handling i samband med detta, på begäran, överlämna handlingen. Detta gäller även när den som är folkbokförd vill ändra uppgift om sin identitet och Skatteverket enligt 23 § andra stycket har begärt att uppgiften ska lämnas vid personlig inställelse. Om den handling som överlämnas innehåller biometriska underlag ska innehavaren låta Skatteverket ta fingeravtryck och ansiktsbild för att kontrollera att dessa motsvarar dem som finns i handlingen. Detta framgår av 26 c §. Det finns alltså stöd för att ta upp biometriska underlag i tre olika situationer enligt folkbokföringslagen. En första fråga är om en identitetsnyckel bör kunna skapas i samtliga dessa fall.

När det gäller flyttning till Sverige för någon som inte tidigare varit folkbokförd här anser vi att det är av stor vikt att en nyckel

skapas, eftersom det är fråga om personer som kommer att bosätta sig i Sverige och få ett personnummer fastställt. En grundidentitet kan behöva etableras vid flyttning till landet. Det kan dock även vara fråga om flyttning till Sverige för personer som varit folkbokförda tidigare, men blivit avregistrerade som utvandrade, och alltså redan har ett personnummer. Även för dessa personer, som kommer att bo i Sverige, anser vi att en identitetsnyckel bör skapas.

En person som är avregistrerad från folkbokföringen som försvunnen ska åter folkbokföras om hans eller hennes rätta vistelseort i Sverige blir känd. Det rör sig om personer som har varit folkbokförda i Sverige och därmed – om ett identitetsindex införs – kan ha registrerats i detta vid något tidigare tillfälle. Behovet av att kunna skapa en identitetsnyckel i ett ärende efter avregistrering skulle därför kunna tänkas vara mindre. Samtidigt kan anledningen till att en person har avregistrerats tala för ett sådant behov. I förarbetena till avskaffandet av möjligheten att bli folkbörd utan känd hemvist anfördes att orsaken till att en person inte vill uppge sin bosättning kan variera. Det kan handla om att man vill hålla sig undan myndigheternas kontroll. Det kan också vara så att man till exempel inte vill tala om var man bor för att detta skulle kunna påverka det bostadsbidrag som den person man sammanbor med får eller för att man har ett andrahandskontrakt och uthyrningen inte är godkänd av fastighetsägaren.[37] Ageranden av det slaget skulle, enligt vår bedömning, kunna motverkas av att en person är registrerad i ett identitetsindex. Att kunna registrera den som har varit avregistrerad som försvunnen i ett identitetsindex, när hans eller hennes vistelseort åter blir känd och ska folkbokföras, anser vi därför är av vikt.

Vad gäller den som vill ändra sina identitetsuppgifter är det också fråga om personer som redan är folkbokförda och som därför på annat sätt kan ha registrerats i ett identitetsindex. Vid ändring av identitetsuppgifterna är det, enligt vår bedömning, av värde att kunna registrera en person som inte tidigare förekommer i ett index, eftersom en ny identitet på sätt och vis etableras. Enligt uppgifter i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* har Skatteverket genomfört en jämförelse av biometriska uppgifter i ett begränsat antal ärenden enligt 23 § andra stycket folkbokföringslagen; år 2022, 2023 och 2024 skedde det endast i 1 110, 946 respek-

[37] *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 32.

tive 1 508 fall.[38] Möjligheten att göra jämförelser av biometriska uppgifter trädde dock i kraft först den 1 september 2023 och enligt uppgifter från Skatteverket saknades tekniskt stöd för att kunna genomföra sådana jämförelser fram till juni 2024. Därefter har antalet kontroller vid personlig inställelse ökat enligt Skatteverket.

Det krävs enlig 23 § andra stycket folkbokföringslagen särskilda skäl för att Skatteverket ska kräva personlig inställelse vid anmälan om ändring av identitetsuppgifter. Av förarbetena till bestämmelsen framgår dels att möjligheten att begära personlig inställelse ska användas sparsamt och endast i fall då det är av väsentlig betydelse för en riktig folkbokföring, dels att en begäran om ändring av identitetsuppgifter rimligen utgör ett sådant fall där personlig inställelse är av väsentlig betydelse för riktig folkbokföring.[39] Det saknas enligt vår bedömning anledning att utgå från annat än att Skatteverket ställer krav på personlig inställelse i de fall när det finns anledning till det. Vi ser därför inte anledning att överväga en förändring av det nuvarande kravet på särskilda skäl, eller vad som ska avses med särskilda skäl, till exempel genom att med sådana skäl bör avses även att en person inte är registrerad i ett identitetsindex. En sådan utökning skulle kunna leda till att en stor mängd personer, i vart fall under en övergångsperiod, skulle vara skyldiga att inställa sig personligen i ärenden där några tvivel om identiteten inte föreligger.

Att registreras i ett identitetsindex i samband med ett ärende om ändring av identitetsuppgifter skulle kunna verka avhållande, vilket kan leda till att en person avstår från att exempelvis rätta felaktiga identitetsuppgifter i folkbokföringen. En sådan effekt bör naturligtvis motverkas. Vi bedömer emellertid att endast omständigheten att en identitetsnyckel också kan skapas i ärendet inte i sig kan antas påverka viljan att ändra identitetsuppgifter i folkbokföringen i någon mer påtaglig utsträckning, Detta med hänsyn till att en registrering i ett index inte kräver någon ytterligare medverkan från den enskilde, utöver vad som redan följer av befintliga bestämmelser i folkbokföringslagen. Till skillnad från gällande ordning där de biometriska underlagen och de uppgifter som tagits fram ur dem omedelbart ska förstöras efter att kontrollen har genomförts, skulle de komma att lagras i ett identitetsindex. Vi kan emellertid notera att enligt förslag som har lämnats i propositionen *Utökade befogenheter för Skatte-*

[38] SOU 2025:75, s. 428.
[39] Jfr prop. 1990/91:153 *om ny folkbokföringslag m.m.*, s. 138 och prop. 2021/22:217, s. 42.

verket inom folkbokföringsverksamheten ska de biometriska underlag som tagits upp vid en identitetskontroll och de biometriska uppgifter som tas fram ur dessa också få lagras av Skatteverket under vissa förutsättningar.[40] Att biometriska uppgifter lagras även i ett identitetsindex medför enligt vår bedömning inte en sådan avhållande effekt att en identitetsnyckel, av det skälet, inte bör kunna skapas i ett ärende om ändring av identitetsuppgifter i folkbokföringen.

Vi anser alltså att en identitetsnyckel bör kunna skapas i samtliga fall då en identitetskontroll genomförs enligt folkbokföringslagen. Som vi noterat ovan är det emellertid inte i alla ärenden som biometriska underlag tas upp vid en sådan identitetskontroll; vid ändring av identitetsuppgifter krävs, enligt 23 § andra stycket, personlig inställelse endast om det finns särskilda skäl, och enligt bestämmelsen i 26 a § andra stycket folkbokföringslagen får Skatteverket, om det finns särskilda skäl, avstå från kravet på personlig inställelse. Med särskilda skäl i 26 a § avses exempelvis att en inflyttande person har kunnat identifieras på annat tillförlitligt sätt eller att personen på grund av sjukdom eller funktionsnedsättning inte kan inställa sig personligen.[41] Vi ser ingen anledning att ändra Skatteverkets möjlighet att, i enlighet med 26 a §, avstå från kravet på personlig inställelse om det finns särskilda skäl. Vi har ovan bedömt att kravet på särskilda skäl i 23 § andra stycket inte bör förändras.

Möjlighet att ta upp biometriska underlag

En grundförutsättning för att en identitetsnyckel ska kunna skapas i något av de ovan nämnda ärendena enligt folkbokföringslagen är att biometriska underlag faktiskt tas upp i samband med en identitetskontroll. Även om det finns ett rättsligt stöd för att ta upp biometriska underlag görs det inte i alla ärenden, bland annat beroende på att det är avhängigt av att anmälaren har ett pass, ett identitetskort eller annan motsvarande handling med ett lagringsmedium där fingeravtryck eller ansiktsbild är lagrade *och* att han eller hon själv upplyser om sitt innehav av en sådan handling. Det kan även vara så att biometriska underlag som finns i en handling inte kan läsas, på grund av att handlingen är skadad eller avläsningsutrustning inte

[40] Prop. 2025/26:261, s. 44 ff.
[41] Prop. 2021/22:217, s. 38.

fungerar. Enligt statistik som redogjordes för i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* hade Skatteverket möjlighet enligt gällande rätt att ta upp biometriska underlag i 144 146 ärenden om inflyttning till Sverige år 2024, men jämförelser med biometriska uppgifter genomfördes endast i cirka 82 000 av dessa.[42]

Som vi anfört i avsnitt 13.2.7 utgår våra förslag i detta kapitel från befintligt, beslutat eller föreslaget rättsligt stöd för att ta upp biometriska underlag. För att öka möjligheten att kunna registrera fler personer i ett identitetsindex i folkbokföringsärenden skulle det därför kunna övervägas att lämna förslag som utökar möjligheterna för Skatteverket att ta upp biometriska underlag i samband med en identitetskontroll. Sådana förslag har emellertid lämnats i propositionen *Utökade befogenheter för Skatteverket i folkbokföringsverksamheten*, genom att en ny i 26 d § folkbokföringslagen som innebär att Skatteverket får möjlighet att ta upp biometriska underlag av en enskild som inställer sig för identitetskontroll oberoende av om den enskilde vid kontrollen har överlämnat en handling enligt 26 b § med ett lagringsmedium där ansiktsbild eller fingeravtryck är sparade. I stället ska det räcka att den identitetshandling som den enskilde överlämnar har en synlig ansiktsbild.[43] Enligt uppgifter från Skatteverket är det emellertid ytterst ovanligt att den som inställer sig personligen för identitetskontroll inte lämnar över en sådan handling. I den stora majoriteten av ärenden kommer det därmed att finnas möjlighet för Skatteverket att ta upp biometriska underlag vid en identitetskontroll enligt folkbokföringslagen. Vidare föreslogs i propositionen att de biometriska underlag som tas upp inte bara ska få kontrolleras mot uppgifter i en överlämnad identitetshandling, utan även jämföras med biometriska uppgifter som Skatteverket och Migrationsverket har lagrat.[44] Vi anser att förslagen effektivt främjar att biometriska underlag kan tas upp i fler folkbokföringsärenden där en identitetskontroll genomförs, och att betydligt fler personer därmed kan fångas upp och registreras i ett identitetsindex.

Mot bakgrund av det ovan anförda anser vi att det, utifrån de personer vi anser bör kunna registreras i ett identitetsindex, finns

[42] SOU 2025:75, s. 417 och 428.
[43] Prop. 2025/26:261, s. 52 ff. och 103.
[44] Se förslag på 26 d och e §§ folkbokföringslagen, prop. 2025/26:261, s. 7.

ett tillräckligt och ändamålsenligt stöd för att ta upp biometriska underlag i ärenden om folkbokföring.

Närmare om när en identitetsnyckel bör kunna skapas

Den fråga som kvarstår är *när* en identitetsnyckel bör skapas i ett folkbokföringsärende. Ett alternativ är att knyta tidpunkten till när en anmälan eller ansökan ges in. Det kan emellertid tänkas att ärendet avskrivs, exempelvis för att utlänningen återtar sin ansökan eller anmälan. Det är inte heller säkert att biometriska underlag tas upp, eftersom det kan finnas särskilda skäl som innebär att personlig inställelse inte krävs i ett enskilt fall. Dessa omständigheter talar mot att en identitetsnyckel bör skapas i ett så tidigt skede. Ett annat alternativ är att, på det sätt som vi bedömt i fråga om anmälan eller ansökan om svenskt medborgarskap, knyta tidpunkten till när de biometriska underlagen tas upp. Ett problem med en sådan lösning är emellertid att det, i ett ärende om folkbokföring av den som inte är folkbokförd, vid den tidpunkten sällan kan anses stå klart att personen ska folkbokföras. Det skulle medföra en risk för att personer som inte kommer att ha en anknytning till Sverige genom att de är folkbokförda här registreras i ett identitetsindex, något som vi anser bör undvikas; dessa personer kommer inte heller att ha något personnummer om de inte tidigare varit folkbokförda, vilket är en uppgift som vi anser bör kunna registreras i identitetsindexet. Även om sådana faktorer inte gör sig gällande på samma sätt i ett ärende om ändring av identitetsuppgifter eller när en person som är avregistrerad från folkbokföringen som försvunnen eller utflyttad åter ska folkbokföras anser vi att en annan tidpunkt bör väljas, om möjligt.

Enligt 26 c § andra stycket folkbokföringslagen ska fingeravtryck och ansiktsbilder samt de biometriska uppgifter som har tagits fram omedelbart förstöras när en kontroll enligt första stycket har genomförts. Förslag om att de biometriska underlagen och de biometriska uppgifterna ska få lagras i de register som Skatteverket för, har emellertid lämnats i den ovan nämnda propositionen *Utökade befogenheter för Skatteverket i folkbokföringsverksamheten*. Detta genom att en ny punkt införs i 1 a § folkbokföringslagen som anger att fingeravtryck, ansiktsbild och de biometriska uppgifter som tas fram ur fingeravtrycken eller bilden ska registreras. Vidare har förslag

lämnats om att 26 c § andra stycket folkbokföringslagen justeras så att bestämmelsen om att fingeravtryck och ansiktsbilder samt de biometriska uppgifter som har tagits fram omedelbart ska förstöras tas bort.[45] Med detta som utgångspunkt skulle det alltså gå att knyta tidpunkten för när en identitetsnyckel skapas till när ärendet avslutas. Vi anser att detta också är lämpligt. Vid den tidpunkten har nödvändiga utredningsåtgärder som främjar korrekta uppgifter i ett index kunnat vidtas, och i ett ärende om inflyttning till Sverige har myndigheten tagit ställning till om personen ska folkbokföras eller inte.

I ärenden som rör ändring av identitetsuppgifter och folkbokföring av den som är avregistrerad som försvunnen eller utflyttad anser vi att en identitetsnyckel bör skapas oavsett utgången i ärendet, eftersom dessa personer redan är eller har varit folkbokförda i landet och därmed kan presumeras ha en sådan anknytning att de bör omfattas av ett index. Vid anmälan om flyttning till Sverige anser vi att motsatt uppfattning bör gälla. En identitetsnyckel bör i de fallen bara skapas om ärendet – antingen genom att Skatteverket beslutar om det i första instans eller efter överklagande – utmynnar i att den enskilde ska folkbokföras i landet. På dessa sätt kan dels personer som blir folkbokförda i landet, dels en viss del av de personer som redan är folkbokförda men som förekommer i ett ärende av sådant slag att lagstiftaren har ansett att identiteten ska utredas genom personlig inställelse fångas upp.

Sammanfattningsvis bör en identitetsnyckel skapas – om biometriska underlag har tagits upp vid en identitetskontroll – för den som folkbokförs efter flyttning till Sverige eller efter att ha varit avregistrerad som försvunnen, och för den som begär ändring av en uppgift om sin identitet.

13.3.7 Ärenden om samordningsnummer

Vår bedömning

En identitetsnyckel bör, om biometriska underlag har tagits upp vid en identitetskontroll, kunna skapas för den som tilldelas ett samordningsnummer, den vars samordningsnummer förnyas, och den som begär ändring av en uppgift om sin identitet.

[45] Prop. 2025/26:261, s. 6 f.

Skatteverket får tilldela samordningsnummer dels efter ansökan från en enskild som har en sådan anknytning till Sverige att han eller hon kan antas behöva en identitetsbeteckning, dels efter begäran från en statlig myndighet – eller vissa enskilda utbildningsanordnare – om samordningsnummer behövs i deras verksamhet.[46] Detta framgår av 2 kap. lagen om samordningsnummer.

Tre nivåer av samordningsnummer

Samordningsnummer förekommer i tre nivåer, beroende på vilken identitetskontroll som föregått tilldelningen av ett sådant nummer: styrkt, sannolik och osäker identitet. Samordningsnummer på identitetsnivå styrkt identitet kräver som utgångspunkt att personen i fråga styrker sin identitet i samband med personlig inställelse hos Skatteverket, eller i praktiken Statens servicecenter. Ett samordningsnummer på identitetsnivå styrkt kan tilldelas både efter ansökan från den enskilde och på begäran av en statlig myndighet. Lagstiftaren har dock resonerat som så att det aldrig bör komma i fråga att tilldela ett samordningsnummer trots att den enskilde inte inställt sig personligen för identitetskontroll när det är den enskilde som ansökt om att tilldelas ett nummer. I dessa fall har den enskilde ett eget intresse av att tilldelas en identitetsbeteckning och det är därför rimligt att i samtliga fall kräva att den enskilde inställer sig personligen och styrker sin identitet, om det inte finns sådana särskilda skäl att Skatteverket avstår från kravet på personlig inställelse.[47]

Samordningsnummer på identitetsnivå sannolik eller osäker kan däremot tilldelas även om den enskilde inte inställer sig personligen, i de fall det är en myndighet som har begärt tilldelning. Huvudregeln är dock att den enskilde ska inställa sig personligen även när tilldelning av samordningsnummer aktualiseras efter begäran från en myndighet. Utgångspunkten är dock att myndigheternas olika behov av samordningsnummer bör tillgodoses. Det behövs därför ett undantag från kravet på styrkt identitet och identitetskontroll vid personlig inställelse, för det fall den enskilde av olika anledningar inte medverkar. Om identiteten inte kan styrkas med godtagbara identitetshandlingar

[46] På begäran av Migrationsverket, Försvarsmakten och Regeringskansliet får samordningsnummer under vissa förutsättningar tilldelas även om myndigheten inte behöver samordningsnumret i sin verksamhet.
[47] Prop. 2021/22:276, s. 77.

eller den enskilde överhuvudtaget inte inställer sig personligen finns det därför en möjlighet för Skatteverket att tilldela samordningsnummer på identitetsnivå sannolik eller osäker.[48]

Möjlighet att ta upp biometriska underlag

Vid en identitetskontroll med personlig inställelse ska den som innehar ett pass, ett identitetskort eller en annan motsvarande handling på begäran överlämna handlingen. Den som har beviljats uppehållstillstånd i Sverige ska på begäran överlämna sitt uppehållstillståndskort. Om en handling som överlämnats har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade, ska innehavaren på begäran låta den myndighet som utför identitetskontrollen ta fingeravtryck och ansiktsbild för att kontrollera att dessa motsvarar dem som finns i handlingen (2 kap. 3 och 4 §§ lagen om samordningsnummer). Under beredningen av bestämmelsen om skyldighet för den som har en identitetshandling med lagrade biometriska data att lämna över den, anfördes att skyldigheten i viss mån är illusorisk eftersom den förutsätter att den enskilde själv upplyser om sitt innehav av en sådan handling. Regeringen ansåg dock att det behövdes en skärpning av regelverket.[49] Tilldelning av samordningsnummer efter ansökan av den enskilde förutsätter dock att den enskilde styrker sin identitet med en identitetshandling, vilket ger incitament att överlämna en identitetshandling till myndigheten.

I propositionen *Utökade befogenheter för Skatteverket i folkbokföringsverksamheten* har förslag lämnats om att Skatteverket ska få möjlighet att ta upp biometriska underlag av en enskild som inställer sig för identitetskontroll oberoende av om den enskilde vid kontrollen har överlämnat en handling enligt 2 kap. 3 § lagen om samordningsnummer med ett lagringsmedium där ansiktsbild eller fingeravtryck är sparade. I stället ska det räcka att den identitetshandling som den enskilde överlämnar har en synlig ansiktsbild.[50] Enligt uppgifter från Skatteverket är det ytterst ovanligt att den som inställer sig personligen för identitetskontroll inte lämnar över en sådan handling. I den stora majoriteten av ärenden kommer det därmed att finnas möjlighet för Skatteverket att ta upp biometriska underlag vid en identi-

[48] A.a., s. 59 f.
[49] Jfr prop. 2021/22:217, s. 44 och 47 samt prop. 2021/22:276, s. 65.
[50] Prop. 2025/26:261, s. 52 f.

tetskontroll enligt lagen om samordningsnummer. Vidare föreslogs i propositionen att de biometriska underlag som tas upp inte bara ska få kontrolleras mot uppgifter i en överlämnad identitetshandling, utan även jämföras med biometriska uppgifter som Skatteverket och Migrationsverket har lagrat.[51] Förslagen främjar att biometriska underlag kan tas upp i fler ärenden om samordningsnummer där en identitetskontroll genomförs och att fler personer då kan registreras i ett identitetsindex.

Mot bakgrund av det ovan anförda anser vi att det, utifrån de personer vi anser bör kunna registreras i ett identitetsindex, finns ett tillräckligt och ändamålsenligt stöd för att ta upp biometriska underlag i ärenden om samordningsnummer.

När en identitetsnyckel bör kunna skapas

Biometriska underlag kan alltså komma att tas upp när den enskilde inställer sig för identitetskontroll i samband med tilldelning av samordningsnummer. Vi bedömer att en identitetsnyckel bör kunna skapas för den som tilldelas ett samordningsnummer oavsett om det är på identitetsnivå styrkt, sannolik eller osäker, under förutsättning att biometriska underlag har tagits upp vid personlig inställelse i samband med identitetskontrollen. I likhet med vad vi anfört ovan om ärenden om inflyttning bör en identitetsnyckel kunna skapas om ärendet – antingen genom att Skatteverket beslutar om det i första instans eller efter överklagande – utmynnar i att den enskilde tilldelas ett samordningsnummer.

Ett samordningsnummer får förnyas efter ansökan av en sådan myndighet som kan begära tilldelning av ett samordningsnummer och efter ansökan av den enskilde. Ett samordningsnummer som vilandeförklarats kan också förnyas. Ett samordningsnummer ska förklaras vilande om inte någon ansökan om förnyelse har kommit in vid utgången av det femte kalenderåret efter det år då numret tilldelades eller senast förnyades eller om det finns andra skäl för det. Vid förnyelse av ett samordningsnummer krävs att förutsättningarna för tilldelning av samordningsnummer i 2 kap. lagen om samordningsnummer är uppfyllda (se 3 kap. 1–3 §§). Den enskilde måste

[51] Se förslag på nya lydelser av 2 kap. 4–4 b §§ lagen om samordningsnummer, prop. 2025/26:261, s. 16 f.

alltså i normalfallet inställa sig personligen och styrka sin identitet. En förnyelse efter ansökan av en enskild kräver – liksom vid tilldelning efter ansökan av en enskild – alltid identitetskontroll vid personlig inställelse, om inte Skatteverket medger undantag från kravet på personlig inställelse (se 2 kap. 2 § andra stycket lagen om samordningsnummer). Om den enskilde inte inställer sig för identitetskontroll eller saknar förmåga att styrka sin identitet men Skatteverket bedömer att förutsättningarna för tilldelning av samordningsnummer på identitetsnivå sannolik är uppfyllda, kan samordningsnumret ändå förnyas och uppgiften som registrerats om identiteten i folkbokföringsdatabasen ändras, till exempel från ”styrkt identitet” till ”sannolik identitet”. En sådan ändring ger en tydlig indikation till myndigheter och privata aktörer att personens identitet vid förnyelsen inte har kontrollerats på ett fullgott sätt genom identitetskontroll vid personlig inställelse.[52]

Även för det fall att en person som har tilldelats ett samordningsnummer vill ändra en uppgift om sin identitet gäller samma bestämmelser som vid tilldelning av samordningsnummer efter styrkt identitet (2 kap. 7 § lagen om samordningsnummer). Detsamma gäller för den som vill ändra den uppgift om bedömningen av identiteten som framgår av folkbokföringsdatabasen. Så kan vara fallet för den som har ett samordningsnummer med uppgift ”sannolik identitet” eller ”osäker identitet” och vill ändra uppgiften till ”styrkt identitet” för att på så sätt öka numrets användbarhet i samhället. Syftet är att säkerställa att den som har tilldelats ett samordningsnummer inte i efterhand ska kunna ändra uppgifterna om sin identitet utan att de nya uppgifterna kontrolleras med samma krav på säkerhet som vid tilldelning av samordningsnummer efter styrkt identitet.[53]

Vi anser att en identitetsnyckel bör kunna skapas även vid förnyelse av ett samordningsnummer och i samband med ett ärende om ändring av identitetsuppgifter för en person som tilldelats ett samordningsnummer, under förutsättning att biometriskt underlag tas upp i samband med identitetskontroll vid personlig inställelse. Identitetsnyckeln bör i sådant fall skapas vid beslut om förnyelse av samordningsnummer respektive vid beslut i ärendet om ändring av identitetsuppgifter. En identitetsnyckel bör kunna skapas i dessa ärenden oavsett om samordningsnumret har tilldelats på styrkt,

[52] Prop. 2021/22:276, s. 143 ff.
[53] A.a., s. 141 f.

sannolik eller osäker identitetsnivå; det avgörande är att biometriska underlag har tagits upp i ärendet.

Sammanfattningsvis bör en identitetsnyckel skapas – om biometriska underlag har tagits upp vid en identitetskontroll, för den som tilldelas ett samordningsnummer, den vars samordningsnummer förnyas, och den som begär ändring av en uppgift om sin identitet.

Särskilt om identitetskontroll hos passmyndighet, beskickning och konsulat

I vissa situationer när tilldelning av samordningsnummer aktualiseras är det inte Skatteverket som genomför identitetskontrollen. När en passmyndighet begär tilldelning av samordningsnummer ska personlig inställelse för identitetskontroll ske vid passmyndigheten[54] och myndigheten ska bedöma om den som ska tilldelas ett samordningsnummer har styrkt sin identitet. Detta framgår av 11 § förordningen (2023:363) om samordningsnummer. Inom riket är Polismyndigheten passmyndighet. Utom riket fullgör beskickningar och karriärkonsulat uppgifter som passmyndighet.[55] En beskickning eller ett karriärkonsulat får också genomföra identitetskontroll av en person som inte befinner sig i Sverige om begäran om tilldelning av samordningsnummer har lämnats av en annan myndighet än en passmyndighet och Skatteverket har begärt att beskickningen eller karriärkonsulatet ska ta emot den enskilde för identitetskontroll (12 § förordningen om samordningsnummer).

Enligt förslag i propositionen *Utökade befogenheter för Skatteverket i folkbokföringsverksamheten* ska Skatteverket lagra de fingeravtryck och den ansiktsbild som den myndighet som genomför en identitetskontroll tar av den enskilde med stöd av 2 kap. 4 § lagen om samordningsnummer, samt de biometriska uppgifter som tas fram ur dessa. När en passmyndighet tar fingeravtryck och ansiktsbild av en enskild vid identitetskontroll i ett ärende om samordningsnummer ska myndigheten, enligt förslagen, lämna uppgifterna till Skatteverket.[56]

[54] Se 3 kap. 7 § Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort (PMFS 2021:3, FAP 530-1).
[55] Se 2 § passlagen (1978:302).
[56] Prop. 2025/26:262, s. 50 och 112.

Det faktum att de biometriska underlag som behövs för identitetskontroll i ett ärende om samordningsnummer i vissa fall tas upp av en annan myndighet än Skatteverket, påverkar enligt vår bedömning inte förutsättningarna för att registrera en person i ett identitetsindex i samband med handläggningen av ett sådant ärende; det är alltjämt Skatteverket som beslutar i ärendet.

Ärenden i vilka biometriska underlag inte tas upp

Biometriska underlag kommer inte att tas upp i samband med en identitetskontroll i ett ärende om samordningsnummer om Skatteverket bedömer att det finns särskilda skäl för att avstå från kravet på personlig inställelse, eller om den enskilde inte inställer sig personligen. Under år 2024 tilldelades cirka 70 000 samordningsnummer och knappt 14 000 nummer förnyades. Drygt 50 000 nummer vilandeförklarades. Av de tilldelade samordningsnumren 2024 var 31 838 på styrkt identitetsnivå, 23 466 på sannolik identitetsnivå och 15 347 på osäker identitetsnivå. Året före, alltså 2023, var dock andelen tilldelade samordningsnummer på sannolik nivå större än styrkt och osäker nivå tillsammans. Vid utgången av år 2024 fanns det totalt cirka 485 000 aktiva samordningsnummer registrerade och cirka 675 000 vilandeförklarade samordningsnummer.[57] Enligt statistik som redogjordes för i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* hade Skatteverket möjlighet att ta upp biometriska underlag i 102 004 ärenden om samordningsnummer år 2024, men jämförelse av biometriska uppgifter genomfördes endast i cirka 19 000 av dessa. Som vi påpekat ovan hade Skatteverket rättslig möjlighet att ta upp biometriska underlag hela år 2024, men teknisk möjlighet infördes först i juni 2024. Andelen kan antas bli större vid utökade möjligheter för Skatteverket att göra kontroller av biometriska uppgifter i enlighet med förslagen i propositionen som vi nämnt ovan.

Det kommer alltså inte att vara möjligt att skapa en identitetsnyckel för personer med samordningsnummer som varken vid tilldelning eller förnyelse av ett sådant nummer inställer sig personligen för identitetskontroll. Därmed kommer det inte heller att vara möjligt för myndigheter som kommer i kontakt med en person som åberopar

[57] *Nationell lägesbild över befolkningen 2025*, dnr 8-174856-2025, Skatteverket, s. 52 f.

samordningsnumret att verifiera identiteten genom kontroll av biometriska uppgifter mot ett identitetsindex. Det innebär i sin tur att det i viss utsträckning fortfarande kommer att vara möjligt att utnyttja samordningsnummer, till exempel för att registrera målvakter i vägtrafikregistret; Transporstyrelsen godkänner identitetsnivån sannolik vid första registrering i vägtrafikregistret och har över 100 000 samordningsnummer registrerade i registret[58].Vi ser dock ingen anledning att frånta Skatteverket möjligheten att avstå från kravet på personlig inställelse om det finns särskilda skäl. Det framstår inte heller som lämpligt att inom ramen för den här utredningen göra personlig inställelse till ett generellt villkor för att ett samordningsnummer ska få tilldelas.[59] Sådana förslag skulle förändra nuvarande system med samordningsnummer i grunden och det är inte möjligt att inom ramen för vårt uppdrag ta ställning till denna fråga.

13.3.8 Ärenden om kvalificerad skyddsidentitet

Vår bedömning

En identitetsnyckel bör kunna skapas för en kvalificerad skyddsidentitet när ett pass eller ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort* utfärdas, om beslutsmyndigheten förordnar om detta i enlighet med 4 § lagen (2006:939) om kvalificerade skyddsidentiteter.

Vid verkställighet av ett beslut om kvalificerad skyddsidentitet bör en kontroll av om personen som tilldelats skyddsidentiteten förekommer i identitetsindexet inte göras.

Vi har tidigare bedömt att det finns ett behov av att kvalificerade skyddsidentiteter omfattas av ett identitetsindex (se avsnitt 12.3.6). Beslut om tilldelning av sådan identitet fattas för Polismyndighetens och Säkerhetspolisens del av Säkerhets- och integritetsskyddsnämnden[60] och meddelas efter ansökan av den myndighet där den som skyddsidentiteten ska avse är anställd. För anställda vid För-

[58] Utredningsuppdrag, Uppdrag att säkerställa att information från folkbokföringen och information om samordningsnummer används ändamålsenligt, dnr TSG 2024-5982, 2025-05-09, s. 15 och 25.
[59] Jfr prop. 2021/22:276, s. 59 ff.
[60] 3 § förordning (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

svarsmakten fattar ett särskilt beslutsorgan inom myndigheten – Försvarsmaktens nämnd för kvalificerade skyddsidentiteter – sådana beslut[61], och när den som skyddsidentiteten ska avse är anställd vid beslutsmyndigheten ska ansökan göras av den enhet inom myndigheten där han eller hon är verksam (5 och 6 §§ lagen om kvalificerade skyddsidentiteter).

Varken Säkerhets- och integritetsskyddsnämnden eller Försvarsmaktens nämnd för kvalificerade skyddsidentiteter – beslutsmyndigheterna – tar upp biometriska underlag vid tilldelning eller förlängning av en skyddsidentitet. I beslut om kvalificerad skyddsidentitet får det emellertid förordnas att Transporstyrelsen ska utfärda körkort i den kvalificerade skyddsidentitetens namn, att andra statliga myndigheter ska utfärda pass eller andra identitetshandlingar i skyddsidentitetens namn eller att Skatteverket ska registrera skyddsidentiteten i folkbokföringsdatabasen. Detta framgår av 4 § lagen om kvalificerade skyddsidentiteter. Biometriska underlag tas upp av Polismyndigheten vid utfärdande av pass. Det är, enligt vår mening, därmed lämpligt att en skyddsidentitet registreras i identitetsindexet och att en identitetsnyckel skapas för skyddsidentiteten när pass utfärdas i skyddsidentitetens namn. Även vid utfärdande av ett sådant statligt identitetskort som föreslagits i promemorian *Ett statligt identitetskort* i skyddsidentiteten kan det enligt vår mening vara lämpligt att registrera skyddsidentiteten i indexet.

Ett beslut om en kvalificerad skyddsidentitet ska verkställas på ett sådant sätt att det inte framgår att det är fråga om en skyddsidentitet (7 § lagen om kvalificerade skyddsidentiteter). I förarbetena anges att det ska framgå av beslutet vilken eller vilka myndigheter som ska verkställa förordnandena i beslutet. Beslutsmyndigheten förutsätts självmant underrätta de berörda myndigheterna om förordnandet och de fiktiva personuppgifter som ska användas. Ytterligare uppgifter, till exempel uppgift om vem som ska använda en skyddsidentitet och till vilken operativ myndighet den är knuten, bör av säkerhetsskäl inte lämnas till de verkställande myndigheterna. Av samma skäl bör en verkställande myndighet inte få del av annat än det förordnande som gäller den myndigheten och inte eventuella ytterligare förordnanden.[62]

[61] Se 28 § förordningen (2024:1333) med instruktion för Försvarsmakten.
[62] *Kvalificerad skyddsidentitet,* prop. 2005/06:149, s. 87.

Vid utfärdande av ett pass eller ett statligt identitetskort för en skyddsidentitet vet Polismyndigheten alltså – genom förordnandet från beslutsmyndigheten – att det är fråga om en skyddsidentitet. Som framgår ovan bör Polismyndigheten dock inte få veta vem som ska använda skyddsidentiteten. Vid utfärdande av ett pass eller identitetskort för en skyddsidentitet bör Polismyndigheten alltså inte identifiera personen som tilldelats skyddsidentiteten med biometriska uppgifter mot ett index för att ta ställning till om det ska skapas en identitetsnyckel för identiteten eller inte. Man skulle kunna tänka sig att Polismyndigheten verifierar skyddsidentiteten med biometriska uppgifter vid utfärdande av en identitetshandling för att kontrollera om skyddsidentiteten har tilldelats en identitetsnyckel. Vi anser dock att den beslutsmyndighet som förordnar om utfärdande av en identitetshandling även behöver ta ställning till om en identitetsnyckel ska skapas i ett identitetsindex i samband med utfärdande av handlingen och förordna om detta när det finns ett behov.

Syftet med en registrering av en skyddsidentitet i ett identitetsindex är primärt att den som tilldelats skyddsidentiteten ska kunna utföra sitt arbete på ett fullgott sätt. Det får enligt vår mening förutsättas att skyddsidentiteten inte kommer att missbrukas och behovet av verifiering från det allmännas sida kan antas vara begränsat. För att undvika att en skyddsidentitet regelmässigt registreras i ett identitetsindex, även när behov av en identitetsnyckel inte kan antas föreligga, anser vi att det bör ankomma på beslutsmyndigheten att ta ställning till registrering. Behov kan till exempel saknas när skyddsidentiteten redan har registrerats i indexet och det finns en identitetsnyckel kopplad till den. Det kan dock även finnas situationer där skyddsidentiteten ska användas på ett sådant sätt att en registrering i ett index inte kan antas fylla någon funktion. Beslutsmyndigheten kan, utifrån information från den myndighet som begär tilldelning av skyddsidentiteten, bäst bedöma behovet av en identitetsnyckel.

Mot den här bakgrunden anser vi att en identitetsnyckel bör kunna skapas för en skyddsidentitet när ett pass eller ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort* (Ju2026/01595) utfärdas, om beslutsmyndigheten förordnar om detta. Genomförande av en sådan lösning skulle enligt vår bedömning förutsätta en ändring i 4 § lagen (2006:939) om kvalificerade skyddsidentiteter.

13.3.9 Andra ärendeslag som kan övervägas

Vår bedömning

En identitetsnyckel bör inte kunna skapas i andra ärendeslag än de vi redogjort för i avsnitt 13.3.1–13.3.8, där biometriska underlag kan tas upp av Polismyndigheten, Migrationsverket (inklusive utlandsmyndigheterna) eller Skatteverket.

För att ett identitetsindex ska kunna få ett ändamålsenligt genomslag behöver så många som möjligt av de personer som ingår i de personkategorier som vi identifierat i kapitel 12 kunna registreras i indexet. Det kan ske på olika sätt, beroende på kategorin. Två huvudsakliga grupper kan urskiljas: de som *redan* tillhör en målgrupp när ett identitetsindex skulle komma att tas i bruk och de som, genom en ansökan eller en anmälan i ett visst ärende, *kommer att* tillhöra målgruppen. Till sistnämnda grupp hör de som beviljas uppehållstillstånd med en giltighetstid som överstiger ett år. Vi bedömer att samtliga dessa personer kommer att kunna fångas upp i ett ärende om utfärdande av uppehållstillståndskort, vilket vi redogjort för i avsnitt 13.3.5. Även de personer som kommer att tillhöra målgruppen med anledning av att de tilldelas ett samordningsnummer eller flyttar till Sverige kommer – under förutsättning att biometriska underlag tas upp – att kunna registreras i ett index i de ärenden vi redogjort för i avsnitt 13.3.6 och 13.3.7. Vad gäller den förstnämnda gruppen, det vill säga de personer som tillhör en målgrupp redan när ett index tas i bruk, bedömer vi att dessa kommer att kunna registreras i ett identitetsindex över tid i varierande omfattning, på följande sätt.

- Den som är svensk medborgare eller blir det genom födelse kommer att kunna registreras i samband med att han eller hon får ett pass eller statligt identitetskort utfärdat. Med hänsyn till den statistik som vi redogjort för i avsnitt 13.3.2 och 13.3.3 kan det antas att upp till två miljoner personer kan fångas upp på detta sätt årligen. Vi bedömer att detta främjar syftet och målet med ett identitetsindex på ett effektivt och ändamålsenligt sätt.
- Den som har uppehållstillstånd med en giltighetstid som överstiger ett år kan registreras i samband med utfärdande av ett nytt uppehållstillståndskort eller – om han eller hon är folkbokförd

eller har tilldelats ett samordningsnummer efter ha att styrkt sin identitet och numret inte är förklarat vilande – vid utfärdande av ett sådant statligt identitetskort utan funktion som resehandling som har föreslagits i promemorian *Ett statligt identitetskort* eller en sådan statlig e-legitimation som har föreslagits i propositionen *En statlig e-legitimation*.[63] Mer sällan kan det också tänkas att en identitetsnyckel kan skapas för den som har ett tidsbegränsat uppehållstillstånd i samband med en anmälan om inflyttning till Sverige. Också den som har permanent uppehållstillstånd kan fångas upp när han eller hon får ett uppehållstillståndskort eller ett statligt identitetskort utfärdat. Giltighetstiden för ett uppehållstillståndskort är begränsad till maximalt tre år eller till den tid som uppehållstillståndet gäller. Vi bedömer därför att tiden för att registrera personer med uppehållstillstånd, efter att ett index skulle komma att tas i bruk, är förhållandevis kort. Den som har permanent uppehållstillstånd kan dessutom registreras i ett index vid en ansökan om svenskt medborgarskap; hur stor andel av de som har permanent uppehållstillstånd som ansöker om svenskt medborgarskap årligen har vi inte kunnat få fram statistik om.

- Den som är folkbokförd i Sverige vid tidpunkten då ett identitetsindex kan tas i bruk, och inte av någon anledning behöver anmäla flyttning till Sverige igen, kommer att kunna registreras i ett index inom ramen för något av de ärenden som vi beskrivit i avsnitt 13.3.1–13.3.5, beroende på om personen är svensk medborgare eller inte.
- Den som har ett samordningsnummer vid tidpunkten då ett identitetsindex tas i bruk kan komma att registreras i indexet vid förnyelse av samordningsnumret eller vid ändring av identitetsuppgifter. En sådan person kan också komma att beviljas uppehållstillstånd med en giltighetstid på minst ett år och i sådant fall registreras i ett index i samband med utfärdande av ett uppehållstillståndskort, eller vid folkbokföring. En utlänning med samordningsnummer på styrkt identitetsnivå, som inte är förklarat vilande, kan också få ett statligt identitetskort utan resefunktion utfärdat, i enlighet med förslag i promemorian *Ett statligt identitetskort*, och registreras i samband med det.

[63] Ju2026/01595 och prop. 2025/26:250.

Mot bakgrund av redogörelsen ovan bedömer vi att en stor majoritet av de personer som vi anser bör omfattas av ett identitetsindex kommer att kunna registreras på ett sätt och inom en tid som innebär att ett sådant system får avsedd effekt och tillräckligt genomslag. För att utöka antalet situationer då olika personkategorier kan bli registrerade, skulle det kunna övervägas att även skapa en identitetsnyckel i andra ärendeslag och situationer där biometriska underlag tas upp. Ett sådant ärendeslag är gränskontroller som görs med stöd av gränskodexen[64] vid inresa till Sverige från tredje land. På det sättet skulle i vart fall fler tredjelandsmedborgare kunna fångas upp.

Vid en inresekontroll tas biometriska underlag upp i olika syften, med stöd av ett flertal bestämmelser i 9 kap. utlänningslagen, bland annat för att kunna kontrollera identiteten genom en jämförelse mot de biometriska underlag som finns lagrade i en handling som utlänningen innehar. Till skillnad från de situationer som har beskrivits i avsnitt 13.3.1–13.3.7 har en gränskontroll mer prägel av faktisk verksamhet än ett ärende, i förvaltningsrättslig mening. Ett ärende karaktäriseras av att det avslutas genom ett beslut av något slag.[65] En gränskontroll kan visserligen utmynna i ett beslut om nekad inresa, men vanligtvis fattas inte något formligt beslut av något slag utan det är endast fråga om att faktiska kontrollåtgärder vidtas. Gränskontroller behöver även kunna genomföras snabbt under en kort tidsrymd, exempelvis på en flygplats, utan att några mer omfattande eller individualiserade utredningsåtgärder vidtas. Det finns numera även en möjlighet att använda så kallad automatiserad gränskontroll i enlighet med artiklarna 8a och 8b i gränskodexen, i form av ett självbetjäningssystem. En registrering i ett identitetsindex behöver, som vi ser det, ske på ett sätt som säkerställer att uppgifterna i så hög utsträckning som möjligt är korrekta från början, och att detta kan kontrolleras när en identitetsnyckel skapas. Detta kan enligt vår mening vara svårt att upprätthålla i praktiken vid en snabb, eller till och med helt automatiserad, gränskontroll.

När en identitetsnyckel skapas är det av vikt att de uppgifter som bör kunna lagras också faktiskt registreras, om möjligt. I avsnitt 11.4.3 och 11.4.4 har vi bedömt att personnummer, samordningsnummer och Migrationsverkets individnummer bör kunna registreras i ett identitetsindex. Särskilt personnumret är av central betydelse vid

[64] Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016.
[65] *Ny förvaltningslag*, prop. 2016/17:180, s. 286.

kontakt med myndigheter och andra aktörer i samhället. Personnummer framgår dock inte av en utländsk resehandling eller av många av de handlingar som kan kontrolleras vid en gränskontroll med stöd av 9 kap. 8 b § utlänningslagen, till exempel ett uppehållskort eller ett permanent uppehållskort. En manuell utredning skulle därför krävas i samband med gränskontrollen för att uppgifter som bör knytas till en identitetsnyckel ska vara så kompletta och korrekta som möjligt. Detta talar enligt vår mening starkt mot att det är lämpligt att en identitetsnyckel skapas vid en inresekontroll. En annan skillnad mot övriga situationer som beskrivs i detta kapitel är att den enskilde inte har sökt upp en myndighet i syfte att ansöka om något, exempelvis ett uppehållstillstånd eller ett pass. Att jämställa en begäran om att få resa in i Sverige med en ansökan om ett pass eller en anmälan om flyttning till Sverige är enligt vår uppfattning svårt att göra.

Mot bakgrund av det ovan anförda anser vi att en identitetsnyckel inte bör skapas vid en inresekontroll enligt gränskodexen.

Vidare bedömer vi att en identitetsnyckel inte heller bör skapas i samband med att Migrationsverket utfärdar ett främlingspass eller ett resedokument för en utlänning i enlighet med 2 kap. 1 a § eller 4 kap. 4 § utlänningslagen. Den personkrets som kan få ett främlingspass eller ett resedokument har sannolikt också uppehållstillstånd och får därmed ett uppehållstillståndskort utfärdat med vissa tidsintervaller, vid vilken tidpunkt personen i fråga kan registreras i ett identitetsindex, om kortet har en giltighetstid på minst ett år.

Enligt förslag i betänkandet *Registrering av EES-medborgare* ska ett särskilt, obligatoriskt, registreringsförfarande för EES-medborgare som vistas i Sverige i mer än tre månader återinföras.[66] I betänkandet föreslogs att Migrationsverket ska få fotografera en EES-medborgare och ta hans eller hennes fingeravtryck i samband med ansökan om registrering av uppehållsrätt, i syfte att verifiera sökandens identitet. Vidare föreslogs att Migrationsverket ska begära ett samordningsnummer hos Skatteverket för en EES-medborgare när han eller hon får ett registreringsbevis utfärdat. Begäran ska dock inte göras om EES-medborgaren är eller har varit folkbokförd eller redan har tilldelats ett samordningsnummer.[67] I betänkandet konstaterades att utredningens förslag medför att de flesta EES-medborgare som ska

[66] SOU 2026:9, s. 119.
[67] A.a., s. 170.

registrera sig behöver genomgå en identitetskontroll vid personlig inställelse både hos Migrationsverket och hos Skatteverket, men att utredningen inte funnit några genomförbara lösningar för att undvika detta.[68]

Mot den här bakgrunden bedömer vi att personkretsen EES-medborgare med uppehållsrätt, som ska registreras hos Migrationsverket i enlighet med förslagen i nämnda betänkande, kommer att kunna registreras i ett identitetsindex inom ramen för det ärende om tilldelning av samordningsnummer som – som utgångspunkt – kommer att inledas av Migrationsverket vid registreringen av EES-medborgaren. Det kan visserligen antas att biometriska underlag i vissa fall inte kommer att tas upp av Skatteverket dessa ärenden (se avsnitt 13.3.7). Även med hänsyn till det bedömer vi att detta, på ett ändamålsenligt sätt och i tillräcklig omfattning, möjliggör att EES-medborgare som vistas i Sverige under mer än tre månader kan fångas upp i ett identitetsindex. I denna bedömning har vi även beaktat att den omständigheten att en person med uppehållsrätt vistas i landet längre än tre månader inte nödvändigtvis innebär att han eller hon också har en sådan anknytning till landet att det finns ett behov av att verifiera identitet mot ett nationellt identitetsindex. Mot denna bakgrund anser vi att en identitetsnyckel inte bör kunna skapas även i ett sådant särskilt ärende om registrering av EES-medborgare som föreslogs i betänkandet *Registrering av EES-medborgare*.

Vi kan i detta sammanhang också notera att förslag i proposition *Åtgärder mot mervärdesskattebedrägerier* har lett till nya bestämmelser i 7 kap. skatteförfarandelagen (2011:1244). Skatteverket får, vid en anmälan om registrering för mervärdesskatt, förelägga en företrädare eller den som anmälan avser att inställa sig personligen om det behövs för kontroll av identitet eller behörighet att företräda den som anmälan avser, och vid sådan kontroll ta fingeravtryck och ansiktsbild för att kontrollera att de motsvarar de uppgifter som finns i pass, identitetskort eller motsvarande handling som den som ska kontrolleras innehar. Syftet är att säkerställa att ytterligare en prövning av identiteten kan göras och att personen är densamma som kan ha kontrollerats av Bolagsverket i samband med en anmälan om registrering till aktiebolagsregistret, och på detta sätt motverka användningen av målvakter samt falska och utnyttjade identiteter. Enligt förarbetena kommer personlig inställelse dock knappast att behöva tillämpas

[68] SOU 2026:9, s. 141.

annat än i undantagsfall, när det av någon särskild anledning behövs för att kontrollera identitet och behörighet.[69] Även om det skulle vara möjligt att på detta sätt fånga upp en liten del av den personkrets som vi anser bör omfattas av ett identitetsindex anser vi att det inte är lämpligt att en identitetsnyckel skapas vid en sådan identitetskontroll som ska få göras med stöd av nya bestämmelser i skatteförfarandelagen.

Inte heller i övrigt anser vi att en identitetsnyckel bör skapas i något ärendeslag som Polismyndigheten, Migrationsverket (inklusive utlandsmyndigheterna) eller Skatteverket handlägger, där biometriska underlag kan tas upp, utöver de som vi redogjort för i avsnitt 13.3.1–13.3.8.

13.4 Ansvar för att skapa en identitetsnyckel

Vi har i avsnitt 13.3 bedömt i vilka ärendeslag som en identitetsnyckel bör kunna skapas. Vi har då emellertid inte närmare berört vilken myndighet som bör ansvara för att faktiskt skapa nyckeln, i de fall det ska göras. I detta avsnitt utvärderar vi vilka myndigheter som bör ansvara för detta.

13.4.1 Ansvaret bör fördelas utifrån ärendeslag

Vår bedömning

En identitetsnyckel bör kunna skapas av den myndighet som beslutar i de ärendeslag som anges i avsnitt 13.3.1–13.3.8.

Den myndighet som bör kunna skapa en identitetsnyckel behöver ha en gedigen organisation, tillräcklig kunskap inom identitetsförvaltning och erforderliga resurser. Därmed kan endast ett fåtal myndigheter komma i fråga. Enligt vår bedömning är det endast Polismyndigheten, Migrationsverket och Skatteverket som är aktuella. Även om utlandsmyndigheterna utfärdar pass och nationella identitetskort, och ska få utfärda det statliga identitetskort som föreslagits i prome-

[69] *Åtgärder mot mervärdesskattebedrägerier*, prop. 2025/26:128, s. 37 ff.

morian *Ett statligt identitetskort*, anser vi, på de skäl som vi redogör för i avsnitt 13.4.2, att de inte bör kunna skapa en identitetsnyckel.

Två huvudsakliga alternativ kan enligt vår bedömning övervägas i fråga om hur ansvaret för att skapa en identitetsnyckel skulle kunna fördelas.

Ett tänkbart alternativ är att fördela ansvaret utifrån ärendeslaget och koppla ansvaret för att skapa en identitetsnyckel till rätten att besluta i ett visst ärendeslag. Utifrån våra bedömningar i avsnitt 13.3 och 13.4.2 kan följande sammanställning av när en identitetsnyckel bör kunna skapas göras.

Tabell 13.4 Ärendeslag där en identitetsnyckel bör kunna skapas

Beslutande myndighet	Ärendeslag
Migrationsverket	Uppehållstillståndskort Svenskt medborgarskap
Skatteverket	Folkbokföring Samordningsnummer
Polismyndigheten	Pass Statligt identitetskort Statlig e-legitimation

Det andra alternativet som kan övervägas är att samla ansvaret för att skapa en identitetsnyckel till en eller vissa angivna myndigheter, eventuellt med utgångspunkt i vilken personkategori som personen som en identitetsnyckel ska skapas för i ett visst fall tillhör. Följande indelning kan då vara lämplig: svenska medborgare, utländska medborgare som har en identitetsbeteckning och utländska medborgare som saknar en identitetsbeteckning.

Vi anser emellertid att ansvaret bör fördelas enligt det första alternativet, av följande skäl. En motsvarighet till ett identitetsindex av det slag vi utvärderar finns inte i Sverige i dag. Att det är fråga om ett helt nytt system innebär att ingen av de tre myndigheter som är aktuella för att skapa en identitetsnyckel har någon specifik erfarenhet som gör den mer eller mindre lämpad för en sådan uppgift. I tidigare lagstiftningsärenden som rör identitetshandlingar och identitetsförvaltning har emellertid bedömts att Polismyndigheten har överlägset större rutin vad gäller att genomföra identitetskontroller i olika ärenden och situationer. Den statistik avseende antal ärenden om utfärdande av pass och nationella identitetskort som utfärdas av

Polismyndigheten respektive identitetskort för folkbokförda som i dag utfärdas av Skatteverket som vi redogjort för i avsnitt 13.3.2 och 13.3.3 ger tydligt stöd för detta. Som vi nämnt ovan i avsnitt 13.3.4 ska Polismyndigheten även ansvara för utfärdande av en sådan statlig e-legitimation som föreslagits i propositionen *En statlig e-legitimation*. I betänkandet *En säker och tillgänglig statlig e-legitimation* lyftes fram att Polismyndigheten har huvudsakligt ansvar för att motverka identitetsrelaterad brottslighet, som en omständighet som med styrka ansågs tala för att denna myndighet bör ansvara för grundidentifieringen vid utfärdande av en statlig e-legitimation.[70] Vi kan vidare notera att i Skatteverkets rapport, *Slutredovisning av regeringsuppdrag att stärka samarbetet för att upprätthålla och sprida kompetens om identitetsfrågor*, föreslogs att ett nationellt ID-center bör vara organiserat inom Polismyndigheten, eftersom myndigheten förfogar över särskild expertkompetens, erfarenhet samt tekniska och organisatoriska resurser för gränskontroll och utfärdande av identitetshandlingar som saknar motsvarighet hos övriga myndigheter, i sammanhanget Skatteverket, Migrationsverket och Statens servicecenter. Det nationella ID-centrets uppdrag och ansvarsområden ska omfatta att samordna, upprätthålla och förmedla kunskap och expertis inom identifiering och dokument samt att samordna utvecklingen av kompetens, metoder och arbetssätt kopplat till identifiering och dokument inom den svenska identitetsförvaltningen.[71]

Polismyndigheten kan alltså anses ha en större erfarenhet av att genomföra identitetskontroller i olika ärenden än i vart fall Skatteverket. Migrationsverket har inte samma erfarenhet vad gäller att utfärda identitetshandlingar men har däremot – enligt vår bedömning – en stor erfarenhet och kunskap vad gäller att bedöma identiteten för olika personkategorier i ärenden där något tydligt beviskrav saknas, vilket kan komplicera bedömningen av identiteten. Polismyndigheten har också en bred erfarenhet av att ta upp och hantera biometriska underlag.

Dessa omständigheter kan enligt vår mening tala för att samla ansvaret för att skapa en identitetsnyckel hos Polismyndigheten, eller möjligtvis hos Migrationsverket. Skapandet av en identitetsnyckel behöver som vi ser det dock inte innefatta några självständiga

[70] SOU 2023:61, s. 177 f.
[71] Slutredovisning, Fi2024/02215, *Att stärka samarbetet för att upprätthålla och sprida kompetens om identitetsfrågor*. Skatteverkets dnr 8-93999-2025, s. 10 och 16.

eller komplexa ställningstaganden i fråga om beviskrav eller handlingars eller uppgifters tillförlitlighet; utredningsåtgärder avseende identiteten och de överväganden som detta kan föranleda görs i så fall inom ramen för det aktuella ärendeslaget, exempelvis en ansökan om pass, om svenskt medborgarskap eller internationellt skydd. Skapandet av en identitetsnyckel blir alltså endast en efterföljande åtgärd och ska inte kräva andra bedömningar än om en viss person redan förekommer i indexet. En sådan bedömning görs – enligt vår bedömning i avsnitt 13.2.1 – genom en biometrisk identifiering, det vill säga genom en datorstödd jämförelse av biometriska uppgifter. Någon särskild kompetens i fråga om att utreda identiteten bör enligt vår uppfattning då inte krävas. Vi anser därför att den stora erfarenhet och kompetens som såväl Polismyndigheten som Migrationsverket ostridigt besitter inte bör ha en avgörande betydelse just i fråga om att skapa en identitetsnyckel. Inte heller den omständigheten att Polismyndigheten – i fråga om platser där biometriska underlag kan tas upp – har en större närvaro i samhället än Skatteverket och Migrationsverket bör enligt vår bedömning ges någon direkt betydelse (pass och nationella identitetskort utfärdas av Polismyndigheten på omkring 110 platser i landet[72] medan Statens servicecenter, när man utför identitetskontroller för Skatteverkets räkning, har möjlighet att ta upp biometriska underlag på 58 servicekontor).[73] Vissa ärendeslag handläggs också utan att personen befinner sig i Sverige, exempelvis ett ärende om uppehållstillstånd som söks innan inresa.

Att samla ansvaret hos en myndighet skulle potentiellt kunna leda till praktiska och rättsliga frågeställningar som i så fall behöver lösas. När det gäller praktiska aspekter skulle en viss individ kunna bli tvungen att uppsöka en annan myndighet än den som beslutar i det ärende som föranleder att en identitetsnyckel ska skapas, om inte den senare ges möjlighet att på något sätt besluta för en annan myndighets räkning i fråga om identitetsnyckeln. Det är enligt vår mening inte svårt att se att en sådan ordning skulle medföra komplexa rättsliga frågeställningar när information – som kan omfattas av sekretess – eventuellt ska föras över till en annan myndighet. Detta inte minst med hänsyn till att biometriska underlag och biometriska uppgifter behöver behandlas i samband med skapandet av en identitetsnyckel,

[72] SOU 2023:61, s. 178.
[73] Statens servicecenter, Årsredovisning 2024, s. 48.

vilket kräver särskilda rättsliga överväganden och säkerhet i processen. Även om skapandet av en identitetsnyckel inte behöver medföra att ett formligt beslut fattas bedömer vi att de åtgärder som vidtas utgör myndighetsutövning. Att exempelvis ge Polismyndigheten ansvar för att skapa en identitetsnyckel i samband med ett ärende om utfärdande av uppehållstillståndskort eller tilldelning av samordningsnummer skulle medföra en uppdelning av myndighetsutövningen på ett sätt som inte framstår som ändamålsenligt, lämpligt eller praktiskt möjlig. Det skulle i vart fall framstå som mycket svåröverskådligt för den enskilde att olika myndigheter agerar i vad som framstår som en och samma process för honom eller henne. Vi menar att en sådan uppdelning kan leda till komplexa gränsdragningsproblem, på liknande sätt som lyftes fram i betänkandet *En säker och tillgänglig statlig e-legitimation* i fråga om en uppdelning av ansvaret för grundidentifiering och utfärdande av en statlig e-legitimation.[74] Vi kan notera att regeringen i beslut från den 27 mars 2025 ändrade den i betänkandet föreslagna uppdelningen och samlade ansvaret hos Polismyndigheten. Regeringen anförde bland annat att samma myndighet bör ha ansvaret för både grundidentifieringen och utfärdandet av den statliga e-legitimationen och att ett sammanhållet myndighetsansvar är mer kostnadseffektivt, minskar administrationen och ökar säkerheten i systemet.[75] Enligt vår mening har dessa faktorer bäring även på den nu aktuella bedömningen.

Sammantaget anser vi att det ovanstående utgör mycket starka skäl mot att peka ut Polismyndigheten, Migrationsverket eller Skatteverket som ensamt ansvarig för att skapa en identitetsnyckel. Det bör inte heller övervägas att fördela ansvaret på några av myndigheterna utifrån vilken personkategori som en viss person tillhör, exempelvis genom att Polismyndigheten ges ansvar för att skapa en identitetsnyckel endast för svenska medborgare och att Migrationsverket ansvarar för utländska medborgare (se dock våra bedömningar i avsnitt 14.4.2 angående fördelning av ansvaret för att rätta eller radera felaktiga uppgifter i ett identitetsindex). En sådan lösning skulle medföra att ansvaret för att besluta i ett visst ärende respektive skapa en identitetsnyckel läggs på olika myndigheter, med risk för samma typ av problematik som lyfts fram ovan. Vi anser i stället

[74] SOU 2023:61, s. 185.
[75] Regeringsbeslut, *Uppdrag att utfärda en statlig e-legitimation på högsta tillitsnivå*, Ju2025/00740, den 27 mars 2025.

att det framstår som naturligt att lägga ansvaret på den myndighet som beslutar i det ärendeslag som föranleder att en nyckel bör kunna skapas. En sådan ordning håller ihop handläggningen på ett tydligt och ändamålsenligt sätt, både praktiskt och rättsligt.

13.4.2 Särskilt om utlandsmyndigheterna

Vår bedömning

Utlandsmyndigheterna bör inte kunna skapa en identitetsnyckel när en sådan myndighet utfärdar ett pass, ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort* eller en sådan statlig e-legitimation som föreslagits i propositionen *En statlig e-legitimation.*

Pass får utfärdas utom riket av utlandsmyndigheter. Detta följer av 2 § tredje stycket passlagen och 3 kap. förordningen (2014:115) med instruktion för utrikesrepresentationen. Pass utfärdas av de utlandsmyndigheter som även är passmyndigheter. Vanliga pass utfärdas emellertid inte av alla utlandsmyndigheter utan endast av dem som har den tekniska utrustningen att ta sökandens fotografi och fingeravtryck. De vanliga passen tillverkas i Sverige och skickas därefter till den utlandsmyndighet där passet ska hämtas ut.[76] Enligt förslag som lämnats i promemorian *Ett statligt identitetskort* ska utlandsmyndigheterna få utfärda även ett statligt identitetskort.[77] I propositionen *En statlig e-legitimation* föreslogs att utom riket bör beskickningar och karriärkonsulat fullgöra uppgifter som utfärdande myndighet av den statliga e-legitimationen i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.[78]

Utlandsmyndigheterna skulle därmed – i de ärenden som vi redogjort för i avsnitt 13.3.2–13.3.4 – som utgångspunkt vara den myndighet som bör kunna skapa en identitetsnyckel, eftersom de beslutar i ärendet och utfärdar den aktuella handlingen. Vi anser emellertid att dessa myndigheter inte bör kunna skapa en identitetsnyckel i samband med handläggningen av ett sådant ärende, på det sätt som Polismyndigheten bör få göra. För det första kan vi konstatera att Sveriges

[76] *Missbruk av svenska pass – Omfattning och åtgärdsförslag*, Ds. 2015:12, s. 72.
[77] Ju2026/01595, s. 63.
[78] Prop. 2025/26:250, s. 43.

utrikesrepresentation består av drygt 100 utlandsmyndigheter. Av dessa är cirka 70 passmyndigheter. Som vi anfört i avsnitt 13.4.1 anser vi att utgångspunkten bör vara att endast ett fåtal myndigheter kan skapa en identitetsnyckel. Möjligheten att kunna registrera uppgifter i system ska som vi ser det vara förbehållet myndigheter som har en gedigen organisation, erforderlig kunskap inom identitetsförvaltning och tillräckliga resurser. Även om det i enstaka fall har konstaterats brister hos utlandsmyndigheter i fråga om bland annat hantering av upptagning av biometriska underlag[79] saknas det enligt vår mening anledning att utgå från annat än att utlandsmyndigheter som är passmyndigheter i sig skulle ha erforderliga förutsättningar för att skapa en identitetsnyckel; som vi anfört i föregående avsnitt innefattar detta i sig inte några bedömningar som kräver särskild kunskap eller erfarenhet.

Vi anser emellertid att det framstår som klart mindre lämpligt ur dataskyddshänseende att ge ett stort antal myndigheter rätt att registrera och – som vi återkommer till i kapitel 14 – uppdatera uppgifter i ett identitetsindex, särskilt som det behöver innehålla biometriska uppgifter. Behandling av känsliga personuppgifter i ett identitetsindex skulle då behöva ske på ett stort antal platser utanför Sverige, många i tredje land. En sådan ordning kan innebära särskilda utmaningar ur tekniskt hänseende för att upprätthålla informationssäkerhet och cybersäkerhet. Det kanske starkaste argumentet mot att en identitetsnyckel bör skapas av utlandsmyndigheterna är emellertid, som vi ser det, den personkrets som dessa myndigheters beslut om att utfärda pass eller identitetshandlingar normalt avser. För det första är det förhållandevis få sådana handlingar som utfärdas av utlandsmyndigheterna, åtminstone sett i ljuset av antalet pass och identitetskort som utfärdas av Polismyndigheten årligen (jämför tabell 13.2 och 13.3).

Tabell 13.5 Utfärdade pass och identitetskort vid utlandsmyndigheterna

År	2020	2021	2022	2023	2024
Antal	28 839	36 557	37 414	35 378	40 005

Källa: Regeringskansliets årsbok 2024, s. 74.

[79] Integritetsskyddsmyndigheten, *Beslut efter tillsyn enligt VIS-, SIS- samt dataskyddsförordningen – Sveriges generalkonsulat i Istanbul*, dnr IMY-2024-2347, den 6 maj 2025.

Att antalet ärenden om att registrera en identitetsnyckel – särskilt sett per utlandsmyndighet – kan antas vara förhållandevis få innebär också att det kan ta lång tid för myndigheterna och den personal som ska hantera sådana ärenden att bygga upp en rutin. Till detta kommer att de personer som ansöker om pass och identitetshandlingar vid en utlandsmyndighet ofta är personer som mer eller mindre tillfälligt vistas utomlands.[80] Vissa av dessa personer kommer därmed inom viss tid att kunna registreras i ett identitetsindex på annat sätt, exempelvis vid flyttning till Sverige eller i samband med att personen förnyar ett pass eller identitetskort i landet, hos Polismyndigheten. För dem som vistas utomlands under längre tid har vi visserligen i avsnitt 12.3.5 bedömt att ett svenskt medborgarskap som sådant medför närmast en presumtion för att det finns en sådan anknytning till Sverige att även personer som är varaktigt bosatta utomlands bör omfattas av den personkrets som kan ingå i identitetsindexet. Vi bedömde samtidigt att behovet av att verifiera identiteten mot ett identitetsindex kan antas vara mindre för dessa personer. Det är vad gäller dessa personer alltså inte fråga om ett behov av att kunna verifiera identitet för en bredare krets aktörer i samhället, som bör tillgodoses i första hand genom ett identitetsindex.

Att inte kunna skapa en identitetsnyckel när utlandsmyndigheter utfärdar ett pass, ett identitetskort eller en särskild statlig e-legitimation kommer alltså endast att innebära att ett förhållandevis begränsat antal personer inte kan fångas upp och registreras i ett index på det sättet. Behovet i sig är därmed inte framträdande. Sett i ljuset av de särskilda tekniska och rättsliga utmaningar som behöver beaktas i fråga om myndigheter som är belägna utanför Sverige anser vi att utlandsmyndigheterna inte bör skapa en identitetsnyckel när de utfärdar ett pass, ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort* eller den statliga e-legitimation som föreslagits i propositionen *En statlig e-legitimation*.[81]

[80] *Passdatalag*, Ds 2015:44, s. 70.
[81] Ju2026/01595 och prop. 2025/26:250.

14 Uppdatering av uppgifter i ett identitetsindex

14.1 Inledning

För att ett register som innehåller personuppgifter eller information av annat slag ska kunna fylla sitt syfte är det naturligtvis av stor vikt att det innehåller riktiga och aktuella uppgifter. Även om ett identitetsindex, enligt våra bedömningar, bör innehålla en begränsad uppsättning uppgifter om de individer som är registrerade i det kan uppgifterna antas behöva uppdateras i olika situationer, exempelvis om någon blir svensk medborgare eller identitetsuppgifterna ändras av annan anledning. I detta kapitel redogör vi närmare för detta.

14.2 Utgångspunkter

En uppdatering av uppgifter i ett identitetsindex kan som vi ser det aktualiseras i två huvudsakliga fall: för att en uppgift har förlorat sin aktualitet (se avsnitt 14.3) eller för att en uppgift är felaktig (14.4). Några gemensamma utgångspunkter kan inledningsvis belysas.

14.2.1 Vad vi avser med att en uppgift uppdateras

Vår bedömning

Med *uppdatering* av en uppgift som behandlas i ett identitetsindex avser vi som utgångspunkt att uppgiften ersätts eller – om den saknas – läggs till. Om en felaktig uppgift inte kan ersättas med en korrekt uppgift kan en uppdatering även innebära att den felaktiga uppgiften raderas.

En fråga som bör belysas redan inledningsvis är vad vi avser med att uppgifter i ett identitetsindex *uppdateras*. Det kan som vi ser det innefatta tre alternativ: att en befintlig uppgift ersätts med en ny, att en ny uppgift läggs till eller att en uppgift raderas.

Vid en sådan uppdatering av uppgifter i ett index som behöver kunna ske löpande på grund av att uppgifterna har blivit inaktuella, på det sätt vi beskriver i avsnitt 14.3, anser vi att de som utgångspunkt ska ersättas med de nya uppgifterna. En sådan ordning har den fördelen att mindre mängder information lagras, vilket är att föredra både ur dataskyddshänseende och ur en teknisk synvinkel.

De alfanumeriska uppgifter som behöver kunna kopplas till en identitetsnyckel är till sin karaktär sådana att de inte kan existera i olika versioner samtidigt; en person kan exempelvis inte ha två olika födelsedatum, namn eller personnummer på samma gång. Det skulle kunna argumenteras för att inte radera de tidigare uppgifterna utan att de tillåts vara kvar i systemet, på det sätt som exempelvis tillämpas i folkbokföringen avseende folkbokföringshistorik, som visar vilka adresser som en person tidigare har varit bosatt på. I folkbokföringsverksamheten sparas även information om tidigare namn som en viss individ har haft och andra identitetsuppgifter. I folkbokföringssammanhang har sådana historiska uppgifter dock ett tydligt syfte. Exempelvis kan uppgifter om under vilken period en person varit folkbokförd på en viss adress ha betydelse i skatterättsliga sammanhang eller för att bedöma om någon haft rätt till ekonomiskt bistånd i egenskap av sammanboende. Vi ser inte samma behov att spara historiska uppgifter i ett identitetsindex, då syftet är att verifiera identitet för en person som en myndighet eller annan aktör möter, utifrån aktuella uppgifter om identiteten och biometriska uppgifter, inte historiska. Verifieringen främjas enligt vår mening inte av att ett identitetsindex innehåller information om att en viss individ tidigare har haft ett annat födelsedatum registrerat eller ett annat efternamn. Sådana uppgifter finns dessutom i många fall tillgängliga i andra register, exempelvis folkbokföringen. Vi har i övrigt inte identifierat något tydligt behov av att behandla även tidigare uppgifter om identitet i ett identitetsindex. Vi gör samma bedömning i fråga om person-, samordnings- och individnummer samt de ansiktsbilder som ska kunna behandlas; om ett identitetsindex innehåller flera olika bilder för en och samma individ skulle det kunna

leda till att en okulär jämförelse blir mer osäker, om flera olika bilder ska bedömas manuellt.

Även biometriska uppgifter bör enligt vår bedömning uppdateras genom att de tidigare ersätts med nya. Det kan visserligen tänkas att om flera biometriska uppgifter lagras skulle det främja en större säkerhet än vad som skulle vara fallet om underlaget var mer begränsat. Ett sådant argument har enligt vår mening emellertid i första hand bäring på om flera *typer* av biometriska underlag och de uppgifter som kan tas fram ur dem finns tillgängliga för jämförelse.[1] Det kan förutsättas att de biometriska uppgifter som behöver kunna lagras i ett identitetsindex håller en tillräcklig kvalitet.

En uppdatering av nämnda uppgiftstyper bör enligt vår bedömning alltså göras genom att befintliga uppgifter ersätts av de nya. Om en viss uppgift helt saknas sedan tidigare – exempelvis för att en person med samordningsnummer blir folkbokförd och får ett personnummer – kan en uppdatering även innebära att nya uppgifter läggs till. Detsamma bör som vi ser det gälla för en uppgift om medborgarskap. I avsnitt 11.4.1 har vi bedömt att samtliga – för svenska myndigheter kända – medborgarskap för en viss individ bör kunna registreras i ett identitetsindex. En uppdatering av medborgarskapet i ett index kan därför innebära såväl att uppgiften ersätts – exempelvis om någon erhåller ett svenskt medborgarskap och det tidigare inte behålls – eller läggs till den befintliga. Sistnämnda situation kan till exempel uppkomma när någon får dubbelt medborgarskap, eller om Migrationsverket vid utredningen av en asylansökan finner anledning att registrera ytterligare medborgarskap för den sökande. Uppgifter om medborgarskap kan också behöva uppdateras genom att ett medborgarskap tas bort.

Som vi nämnt i föregående avsnitt kan en uppgift i vissa fall behöva raderas, nämligen om den är objektivt felaktig men det saknas korrekta uppgifter att ersätta den med. En uppdatering kan därför, i sådana situationer, också innebära att en uppgift raderas (se avsnitt 14.4).

[1] Jfr *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 424.

14.2.2 Vikten av objektivt korrekta uppgifter

De bedömningar vi gör i avsnitt 14.3 syftar till att uppgifter som behandlas i ett identitetsindex behöver kunna uppdateras i vissa givna situationer för att de ska vara aktuella. Det är då helt givet att den uppgift som ska ersätta en befintlig uppgift objektivt ska vara riktig, inte endast i ljuset av det ändamål som den behandlas i ett identitetsindex för och de verkliga förhållanden som den ska återspegla. Som vi återkommer till i avsnitt 14.4 är en grundförutsättning för att en rättelse enligt dataskyddsförordningen[2] ska kunna göras också att en felaktig uppgift kan ersättas med en korrekt uppgift (jfr Högsta förvaltningsdomstolens avgörande, HFD 2019 ref. 9).

Att den uppgift som ska användas för att uppdatera ett identitetsindex är objektivt korrekt får emellertid säkerställas i annan ordning, med tillämpning av de krav på myndigheter att utreda ett ärende som kan följa av allmänna principer i 23 § förvaltningslagen (2017:900) eller av en utökad utredningsskyldighet i ett visst ärendeslag. Beviskrav som eventuellt kan gälla i ett visst ärende får också betydelse. Exempelvis ställs vid en begäran om ändring av identitetsuppgifter i folkbokföringen krav på att den enskilde lägger fram bevisning som innebär att det *klart framgår* att de nya uppgifterna är riktiga (se nyss nämnda avgörande från Högsta förvaltningsdomstolen). Vid ändring av uppgifter i folkbokföringen som en följd av att någon har ansökt om namnbyte med tillämpning av namnlagen finns å andra sidan normalt inte anledning att betvivla ”riktigheten” i uppgifterna; om ansökan beviljas är det nya namnet per definition korrekt. Även vid ändring av ett person- eller samordningsnummer som beror på att den enskilde har bytt juridiskt kön saknas skäl att ifrågasätta de ändrade uppgifterna i sig. Identitetsuppgifter, särskilt i fråga om födelsetid, kan i vissa fall komma att ändras inom ramen för ett ärende om medborgarskap genom naturalisation. De beviskrav som gäller för den ärendetypen – som utgångspunkt att identiteten ska styrkas men att det i vissa fall kan räcka att den görs sannolik – kommer då att vara avgörande; hur ändrade uppgifter om identiteten har bedömts i praxis, se bland annat Migrationsöverdomstolens avgöranden MIG 2019:18, MIG 2023:7 och MIG 2024:6.

Om biometriska uppgifter eller en ansiktsbild uppdateras ankommer det på den myndighet som uppdaterar uppgiften i ett identi-

[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

tets-index att kontrollera att den är av sådan kvalitet som systemet förutsätter. Med hänsyn till att vi i avsnitt 14.3 gör bedömningen att en uppdatering av nämnda typer av uppgifter, i syfte att hålla dem aktuella, bör göras i de ärendeslag som vi redogjort för i kapitel 13 kan detta inte antas innebära några problem i praktiken. En kontroll av att underlagen och uppgifterna är av tillräcklig kvalitet kan även göras indirekt, genom att en biometrisk verifiering görs mot ett identitetsindex innan sådana uppgifter uppdateras.

14.3 Uppdatering för att uppgifter ska vara aktuella

Att de uppgifter som behandlas i ett identitetsindex ska vara korrekta följer inte bara av att detta är en förutsättning för att tillförlitligheten till ett sådant system ska kunna bibehållas utan även av principen om riktighet i artikel 5.1 d dataskyddsförordningen. Av bestämmelsen framgår att alla rimliga åtgärder ska vidtas för att säkerställa att personuppgifter, som är felaktiga i förhållande till de ändamål för vilka de behandlas, raderas eller rättas utan dröjsmål. Det åligger den personuppgiftsansvarige att självmant vidta sådana åtgärder. En personuppgift är felaktig om den inte stämmer överens med verkliga förhållanden. Vad som utgör de verkliga förhållanden som en viss uppgift ska spegla får avgöras utifrån ändamålet för behandlingen av personuppgiften (se EU-domstolens dom i mål C-434/16, *Nowak*). Även bedömningen av hur ofta en uppgift behöver uppdateras för att vara riktig avgörs utifrån det ändamål som den behandlas för. Uppdateringen av de behandlade uppgifterna utgör enligt EU-domstolen en väsentlig aspekt av skyddet för den registrerade med avseende på behandlingen av personuppgifter (se domstolens dom i mål C-247/23, *VP mot Országos Idegenrendészeti Foigazgatóság*). Mot denna bakgrund måste det säkerställas att uppgifterna i ett identitetsindex kan hållas uppdaterade när de verkliga förhållanden som de ska återspegla förändras.

För att en uppgift i ett identitetsindex ska anses riktig i den mening som avses i artikel 5.1 d dataskyddsförordningen måste uppgiften alltså – med hänsyn till ändamålet med behandlingen – återspegla de verkliga förhållandena vid varje givet tillfälle då en verifiering eller identifiering mot ett index görs. Vad detta närmare innebär i förhållande till de uppgifter som ska få behandlas varierar med typen

av uppgift. Bedömningen får göras i ljuset av det ändamål som respektive uppgiftstyp behandlas för i ett identitetsindex, det vill säga att stärka möjligheterna att verifiera identitet i olika sammanhang, med hjälp av biometriska uppgifter. I detta avsnitt tar vi ställning till när de typer av uppgifter som ska få behandlas i ett identitetsindex bör uppdateras, på grund av att de kan anses ha förlorat sin aktualitet och därför inte längre kan betraktas som korrekta. Det är inte möjligt att på förhand förutse exakt *när* detta kommer att ske. Det är emellertid av vikt att uppdateringar, och därmed behandling av personuppgifter, inte görs i onödan, och att en reglering av när en uppdatering i ett identitetsindex bör göras präglas av dels förutsebart, dels tydlighet. Regleringen bör också så långt som möjligt säkerställa att principen om riktighet i dataskyddsförordningen upprätthålls.

14.3.1 Översiktlig bedömning av när uppgifter bör uppdateras

Det är endast en begränsad uppsättning uppgifter som, enligt våra överväganden i kapitel 11, bör få behandlas i ett identitetsindex. Uppgifterna är inte heller av sådant slag att de normalt sett kan antas kräva mer frekventa uppdateringar på grund av att de har förlorat sin aktualitet, vilket kan vara fallet i ett register vars innehåll utgörs av information som kontinuerligt och med korta intervaller tillförs från andra källor.

För det första kan vi konstatera att en alfanumerisk identitetsnyckel av naturliga skäl aldrig behöver uppdateras. Uppgifter om identitetsbeteckning, det vill säga personnummer och samordningsnummer, och Migrationsverkets individnummer, kan behöva uppdateras endast i undantagsfall. Enligt vår bedömning rör det sig i praktiken endast om situationer där en person ändrar juridiskt kön, vilket innebär att person- eller samordningsnumret ändras. Uppgifter om personnummer kan däremot behöva uppdateras för den som har tilldelats ett samordningsnummer och som därefter folkbokförs. I avsnitt 14.3.4 och 14.3.5 gör vi bedömningar avseende i vilka situationer dessa typer av uppgifter bör uppdateras. Uppgifter om identitet kan också ändras, exempelvis vid ett namnbyte i samband med giftermål eller när ett medborgarskap ändras. En uppdatering kan då behöva ske i identitetsindexet (se avsnitt 14.3.2). När det gäller ansiktsbild kan en sådan uppgift behöva uppdateras med vissa inter-

vall både för vuxna och barn, i syfte att kunna upprätthålla möjligheten till en verifiering av identitet genom en okulär jämförelse. Behovet kan antas vara mer framträdande för barn. Eftersom biometriska uppgifter som har tagits fram ur ansiktsbilden ska kunna användas för en datorstödd jämförelse anser vi att det är av stor vikt att det finns ett aktuellt jämförelsematerial; en uppdatering av sådana uppgifter med vissa intervall bör därför övervägas. Vi återkommer till detta i avsnitt 14.3.6. Våra bedömningar kring när olika slags uppgifter i ett index bör uppdateras på grund av att de kan ha förlorat sin aktualitet kan redan här sammanfattas enligt följande.

Tabell 14.1 Översikt av när inaktuella uppgifter i indexet bör uppdateras

En uppgift om	Bör uppdateras av	När
Identitet för personer med identitetsbeteckning Personnummer Samordningsnummer Sekretessmarkering	Skatteverket	Ändring görs i folkbokföringsverksamheten
Identitet för personer som saknar identitetsbeteckning Individnummer	Migrationsverket	Ändring görs i den centrala utlänningsdatabasen
Ansiktsbild Biometriska uppgifter	Den myndighet som tar upp biometriska underlag och som skulle ha skapat en identitetsnyckel	I ett ärende om – pass – statligt id-kort – statlig e-legitimation – uppehållstillståndskort – svenskt medborgarskap – folkbokföring – samordningsnummer

14.3.2 Identitetsuppgifter

Vår bedömning

En uppgift om identitet – det vill säga namn, födelsetid och medborgarskap – i ett identitetsindex bör uppdateras av Skatteverket när myndigheten ändrar en sådan uppgift i folkbokföringen. För den som saknar identitetsbeteckning bör Migrationsverket uppdatera en uppgift om identitet när myndigheten ändrar en sådan uppgift för honom eller henne i den centrala utlänningsdatabasen.

Uppgifter om identitet är centrala inte bara i ett identitetsindex utan också i befintliga register som Polismyndigheten, Migrationsverket och Skatteverket för, exempelvis folkbokföringsverksamheten och den centrala utlänningsdatabasen. Dessa register har en central roll i att lagra och förmedla information om individer som av olika anledningar har en anknytning till Sverige.

Uppgifterna i folkbokföringsverksamheten distribueras till andra offentliga aktörer i samhället genom Navet (Skatteverkets system för distribution av folkbokföringsuppgifter till samhället), och till övriga delar av samhället genom SPAR (Statens personadressregister). Uppgifterna hålls aktuella genom att ändringar i folkbokföringen slår igenom direkt i Navet och genom att SPAR uppdateras varje dag med nya uppgifter från folkbokföringen. Ett identitetsindex skulle enligt vår mening, när det gäller verifiering av identitet, potentiellt kunna få samma centrala och betydelsefulla roll i samhället som Navet och SPAR. Med hänsyn till detta framstår det som naturligt att uppgifter om identitet i ett identitetsindex bör kunna uppdateras på samma sätt som Navet och SPAR, det vill säga att när en ändring sker av en individs identitetsuppgifter i folkbokföringsdatabasen ska det även direkt återspeglas i indexet. Detta säkerställer att samma uppgifter i fråga om identitet för en viss individ förekommer i samtliga dessa system. Motsvarande bör gälla i förhållande till den centrala utlänningsdatabasen för personer som saknar identitetsbeteckning.

Mot bakgrund av det ovanstående anser vi att de verkliga förhållanden som uppgifter om identitet i ett index behöver stämma överens med utgörs av motsvarande uppgifter om identitet som är registrerade för en viss individ i folkbokföringsverksamheten eller – för personer som saknar identitetsbeteckning – den centrala utlänningsdatabasen.

I sistnämnda grupp ingår främst personer som innan inresa har fått ett uppehållstillståndskort med en giltighetstid som överstiger ett år utfärdat och som inte har flyttat till Sverige och blivit folkbokförda. I undantagsfall kan även personer som har ställning som varaktigt bosatta i Sverige komma att omfattas (se avsnitt 12.3.4). En viss identitetsuppgift riskerar med dessa utgångspunkter därför att vara inaktuell, och därmed oriktig, först *efter* det att en ändring gjorts i folkbokföringen eller centrala utlänningsdatabasen. Att det innan den tidpunkten kan ha kommit fram omständigheter som talar för att tidigare uppgifter inte är de korrekta förändrar inte bedömningen; det krävs som vi ser det att bedömningen av de nya uppgifterna också har manifesterats på något sätt – i detta fall genom att Skatteverket eller Migrationsverket ändrar uppgifterna i respektive register.

Möjligheten till identitetskontroll och andra utredningsåtgärder, samt de beviskrav som följer av praxis (se HFD 2019 ref. 9) vid ändring av identitetsuppgifter i folkbokföringsdatabasen, främjar en stabilitet i folkbokföringen. Genom att knyta tidpunkten för en uppdatering av sådana uppgifter i ett identitetsindex till Skatteverkets åtgärder i folkbokföringen, kan en motsvarande stabilitet i ett identitetsindex främjas för personer med en identitetsbeteckning.

En ändring kan ske av olika anledningar. Det kan vara på Skatteverkets initiativ enligt 31 § folkbokföringslagen (1991:481), som en följd av en tillämpning av lagen (2016:1013) om personnamn eller efter en anmälan från den enskilde. Det kan också ske efter en underrättelse från någon annan myndighet; enligt 32 c § folkbokföringslagen respektive 4 kap. 1 § lagen (2022:1697) om samordningsnummer ska en myndighet underrätta Skatteverkets folkbokföringsverksamhet om det kan antas att en uppgift i folkbokföringen om en person som är eller har varit folkbokförd eller har tilldelats ett samordningsnummer är oriktig eller ofullständig. En tänkbar situation är att Migrationsverket i sina ärendehanteringssystem ändrar en uppgift om födelsetid för en viss person, som av något skäl har ett personnummer eller ett samordningsnummer, exempelvis med anledning av att personen tidigare har vistats i landet med uppehållstillstånd på annan grund. Oavsett anledningen till det görs ändringen i folkbokföringsverksamheten av Skatteverket. Vi anser därför att det är lämpligt att denna myndighet uppdaterar ett identitetsindex i sådana situationer. På så sätt ansvarar en och samma myndighet för att upp-

datera uppgifter om identiteten för personer som förekommer både i folkbokföringen och i ett identitetsindex.

För personer som saknar en identitetsbeteckning är det däremot inte möjligt att knyta uppdateringstidpunkten till en åtgärd av Skatteverket. En ändring av identitetsuppgifter för en dessa personer behöver inte nödvändigtvis vara knuten till ett beslut av Migrationsverket utan kan föranledas av utredningsåtgärder som vidtagits i exempelvis ett ärende om uppehållstillstånd; det kan röra sig om att sökanden har kommit in med nya identitetshandlingar eller att en ambassadförfrågan har genererat ny information om identiteten. Förutom när de nya uppgifterna kan få omedelbara konsekvenser – exempelvis om en sökandes ålder justeras så att han eller hon bedöms som vuxen i stället för barn – kommer ändrade bedömningar i fråga om medborgarskap eller födelsetid för en sökande dock ofta till uttryck först i samband med ett beslut i ärendet om uppehållstillstånd. En ändring av sådana uppgifter kan också vara ett resultat av ett avgörande från domstol efter överklagande av Migrationsverkets beslut. Gemensamt för dessa situationer är att de leder till en ändring i den centrala utlänningsdatabasen, inte i folkbokföringen. Med hänsyn till detta anser vi att för personer som saknar ett person- eller samordningsnummer bör en uppdatering av uppgifter om identitet i ett identitetsindex göras av Migrationsverket när myndigheten ändrar en sådan uppgift för honom eller henne i den centrala utlänningsdatabasen.

För att säkerställa att en ändring av en uppgift om identitet i folkbokföringen eller den centrala utlänningsdatabasen får genomslag i ett identitetsindex anser vi att en uppdatering *alltid* bör göras i dessa fall. Att överlåta till Skatteverket och Migrationsverket att i det enskilda fallet ta ställning till om en uppdatering bör göras skulle medföra en risk för att uppgifterna i ett index inte kommer att stämma överens med verkliga förhållanden på det sätt vi redogjort för ovan.

14.3.3 Särskilt om sekretessmarkering

Vår bedömning

När Skatteverket för in eller tar bort en sekretessmarkering för en person i folkbokföringen bör myndigheten uppdatera ett identitetsindex på motsvarande sätt.

I avsnitt 13.2.2 har vi föreslagit att en markering bör göras i identitetsindexet när en identitetsnyckel skapas, om det i folkbokföringen finns en sekretessmarkering för individen i fråga. På samma sätt som när identitetsuppgifter ändras i folkbokföringen anser vi att det är av vikt att en sekretessmarkering återspeglas i ett index. Både när en sådan markering förs in i folkbokföringen och när den eventuellt tas bort, bör det alltså medföra en motsvarande uppdatering i ett index, på samma sätt som görs i SPAR. Det är endast Skatteverket som kan registrera en sekretessmarkering i folkbokföringen. För att säkerställa att en ändring av en sekretessmarkering i folkbokföringsdatabasen får genomslag i identitetsindexet anser vi att en uppdatering *alltid* bör göras i dessa fall. Att överlåta till Skatteverket att besluta i det enskilda fallet om en uppdatering bör göras skulle medföra en risk för att uppgifter om namn i ett identitetsindex felaktigt lämnas ut, eller att de inte görs tillgängliga trots att en sekretessmarkering har tagits bort i folkbokföringen.

14.3.4 Person- och samordningsnummer

Vår bedömning

En uppgift om person- eller samordningsnummer i ett identitetsindex bör uppdateras av Skatteverket när myndigheten ändrar en sådan uppgift i folkbokföringen.

Person- och samordningsnummer är i likhet med identitetsuppgifter av central betydelse i den svenska identitetsförvaltningen och för att den enskilde ska kunna ta del av olika funktioner i samhället. Vad vi anfört i föregående avsnitt om hur identitetsuppgifter i folkbokföringen förmedlas till Navet och till SPAR har enligt vår bedömning

bäring även på en identitetsbeteckning. Vi anser därför att de verkliga förhållanden som uppgifter i ett identitetsindex om person- och samordningsnummer ska återspegla utgörs av motsvarande uppgifter i folkbokföringen. En identitetsbeteckning riskerar därför att vara inaktuell, och därmed oriktig, först *efter* det att en ändring gjorts i folkbokföringen.

Ett personnummer är unikt och följer normalt samma individ under hela livet. Det ändras inte om någon till exempel flyttar utomlands och registreras som utflyttad. Ett samordningsnummer ersätts däremot av ett personnummer om personen folkbokförs i Sverige. Under vissa förutsättningar – om födelsetiden ändras eller en person byter juridiskt kön – kan ett person- eller samordningsnummer också behöva ändras, men då endast efter ansökan från den enskilde och beslut av Skatteverket. Att en uppgift om födelsetid eventuellt ändras inom ramen för ett ärende hos Migrationsverket eller hos en annan myndighet innebär inte att ett person- eller samordningsnummer ändras per automatik. I stället kan en skyldighet att underrätta Skatteverket om detta uppkomma enligt 32 c § folkbokföringslagen. Det är då Skatteverket som ska ändra uppgifterna i folkbokföringsverksamheten. Även om en identitetsbeteckning därmed kan antas ändras endast i få fall bör en ändring av sådana uppgifter i folkbokföringen naturligtvis återspeglas i ett identitetsindex så snart som möjligt. Detta också med hänsyn till att dessa identitetsbeteckningar kan användas som alfanumeriska sökbegrepp för att lokalisera en individ i ett index, eftersom de är unika (se avsnitt 18.3.1).

Vi anser mot denna bakgrund att en uppgift om identitetsbeteckning bör uppdateras i ett identitetsindex när Skatteverket ändrar sådana uppgifter i folkbokföringsverksamheten, på samma sätt som för identitetsuppgifter. Med ändring avses enligt vår bedömning både att en person tilldelas en ny identitetsbeteckning och att ett befintligt person- eller samordningsnummer ändras. I likhet med vår bedömning i avsnitt 14.3.2 behöver en uppdatering *alltid* göras av uppgifterna i ett identitetsindex; det bör alltså inte ankomma på myndigheten själv att avgöra om så ska ske i det enskilda fallet.

14.3.5 Migrationsverkets individnummer

Vår bedömning

En uppgift om individnummer i ett identitetsindex bör uppdateras av Migrationsverket när myndigheten ändrar en sådan uppgift i den centrala utlänningsdatabasen.

När en person för första gången blir aktuell i ett ärende hos Migrationsverket skapas ett unikt individnummer (dossiernummer).[3] Individnumret förekommer i första hand i ärenden hos Migrationsverket men används även för att identifiera en utlänning i ärenden hos Polismyndigheten och i mål hos domstolarna. Individnumret följer individen i olika ärenden hos Migrationsverket och ändras, enligt den information vi fått av företrädare för myndigheten, normalt sett inte. Individnumret har visserligen inte samma spridning i samhället som uppgifter om identitet eller person- och samordningsnummer, men kan på samma sätt som en sådan identitetsbeteckning få betydelse för att identifiera en utlänning i olika sammanhang. Ett individnummer bör enligt vår bedömning också att kunna användas som ett alfanumeriskt sökbegrepp för att lokalisera en individ i ett identitetsindex, eftersom det är unikt (se avsnitt 18.3.1).

Individnumret används, som sagt, framför allt i Migrationsverkets verksamhet. Det är denna myndighet som eventuellt beslutar om en ändring av en sådan uppgift. Ändringen görs då i den centrala utlänningsdatabasen och det är från detta register som uppgiften hämtas av andra system och myndigheter. Vi anser med hänsyn till detta att det verkliga förhållande som en uppgift om individnummer för en viss individ i ett identitetsindex ska spegla är motsvarande uppgift i den centrala utlänningsdatabasen. För att kunna hålla en uppgift om individnummer i ett index aktuell anser vi därför att en uppdatering bör göras av Migrationsverket när myndigheten ändrar en sådan uppgift i den centrala utlänningsdatabasen. I likhet med vad som anförts angående identitetsuppgifter för personer med en identitetsbeteckning i avsnitt 14.3.2 innebär detta att samma myndighet kommer att ansvara för att uppdatera uppgifter om individnummer både i den centrala utlänningsdatabasen och i ett index. Härigenom motverkas att eventuella felaktigheter uppstår av misstag eller att en uppdater-

[3] *Säkerhetsskyddslagen – ytterligare kompletteringar*, SOU 2025:42, s. 241.

ing faller bort. Att samma myndighet ansvarar för ändringen respektive uppdateringen har även effektivitetsfördelar.

Omständigheter som talar i annan riktning än att en uppdatering *alltid* bör ske när en ändring görs i den centrala utlänningsdatabasen har inte kommit fram.

14.3.6 Ansiktsbild och biometriska uppgifter

Vår bedömning

Ansiktsbild och biometriska uppgifter som tagits fram ur den bör uppdateras i ett identitetsindex av Polismyndigheten, Migrationsverket och Skatteverket i samma ärenden som en identitetsnyckel hade kunnat skapas.

Ett identitetsindex syftar till att olika aktörer ska kunna använda biometriska uppgifter för att verifiera identitet i större utsträckning än vad som är möjligt i dag. Som vi anfört i avsnitt 14.3.1 kan ansiktsbilder och biometriska uppgifter behöva uppdateras med vissa intervall, både för vuxna och barn. De verkliga förhållanden som sådana uppgifter ska återspegla är, enligt vår bedömning, de fysiska kännetecken som den individ som uppgifterna är kopplade till i ett identitetsindex har vid ett givet tillfälle. Om exempelvis ansiktsbilden för en viss individ föreställer ett yngre barn men personen vid verifieringstillfället är vuxen, kan uppgiften svårligen anses spegla de verkliga förhållandena, varken i objektiv mening eller sett i ljuset av det ändamål för vilket den behandlas. Detsamma gäller vid sådana förhållanden för biometriska uppgifter som tagits fram ur ansiktsbilden och lagrats i ett identitetsindex.

Till skillnad från vad som gäller för de alfanumeriska uppgifter som vi redogjort för i avsnitt 14.3.2–14.3.5 är det inte möjligt att knyta tidpunkten för *när* en viss ansiktsbild eller biometrisk uppgift som behandlas i ett identitetsindex blir inaktuell till någon viss objektiv åtgärd. Med hänsyn till att en viss persons fysiska kännetecken normalt kan förändras över tid blir det i stället fråga om att kunna bestämma ett lämpligt, generellt, intervall som så långt som möjligt säkerställer att uppgifterna vid varje givet tillfälle är att betrakta som riktiga. Det bör understrykas att endast den omständig-

heten att en persons fysiska kännetecken förändras inte nödvändigtvis innebär att de biometriska uppgifterna inte kan användas för att verifiera identitet, vilket alltså talar för att de alltjämt skulle vara riktiga i den mening som avses i artikel 5.1 d i dataskyddsförordningen. I detta sammanhang bör särskilt beaktas att utgångspunkten vid behandling av personuppgifter – och särskilt känsliga sådana – är att behandling endast ska ske i den utsträckning som är nödvändig. Även med hänsyn till detta anser vi att det är av central vikt för att ett identitetsindex ska fylla sitt syfte att det vid varje givet tillfälle finns ett så uppdaterat biometriskt jämförelsematerial som möjligt. Som vi återkommer till nedan anser vi också att uppdateringen bör ske i samband med att biometriska underlag tas upp av annan anledning; en ytterligare upptagning ska alltså inte krävas för att uppdatera ett index.

Frågan är alltså med vilka intervall en uppdatering av den ansiktsbild och de biometriska uppgifter som är lagrade i ett identitetsindex bör ske, för att upprätthålla principen om riktighet men utan att sådana uppgifter behandlas i onödan. Vi gör följande överväganden.

Möjliga intervall

När det gäller ansiktsbilder är bedömningen av hur ofta de bör uppdateras till stor del knuten till åldern på individen. En ansiktsbild och de biometriska uppgifter som tagits fram ur den anses kunna ge tillräckligt tillförlitligt underlag för jämförelse för en vuxen under cirka tio år. Den fysiska utvecklingen som särskilt yngre barn genomgår gör däremot att en lagrad ansiktsbild efter kort tid blir inaktuell. Som generell riktlinje över hur ofta barns ansiktsbilder behöver uppdateras på grund av fysiska ändringar eller åldrande har sagts att det för närvarande för spädbarn behöver ske efter veckor, för barn efter två år och för ungdomar efter fem år.[4] I förarbetena till 3 § passlagen (1978:302) bedömdes en giltighetstid om tre år för pass till barn som inte fyllt tolv år innebära att problemet med att barns utseende förändras i förhållande till fotografiet i passet minskar.[5] Enligt vår bedömning bör endast barn som har fyllt sex år omfattas av den personkrets som kan ingå i ett identitetsindex. Med hänsyn

[4] Publikation från IOM UN Migration – *Legal Identity Unit*, *Introduction to Biometrics*, s. 26.
[5] *Åtgärder mot missbruk av svenska pass*, prop. 2015/16:81, s. 20 f.

till yngre personers begränsade rättshandlingsförmåga kan det dock med fog antas att det främst är ungdomar som kommer att behöva verifiera sin identitet mot ett identitetsindex (se avsnitt 12.4.1).

Mot denna bakgrund kan vi konstatera att lämpliga intervall för en ansiktsbild och de biometriska uppgifter som tagits fram ur den skulle kunna vara allt mellan tre och tio år, utan att tillförlitligheten i dem som jämförelsematerial går förlorad. Ett intervall om tio år framstår däremot som alltför stort; bland annat i förslag om ett statligt identitetskort anfördes att en begränsning av giltighetstiden för en sådan handling till fem år är av stor betydelse ur ett säkerhetsperspektiv, eftersom innehavarens utseende inte hinner förändras i så stor utsträckning under giltighetstiden.[6] Vi delar denna bedömning. Vi anser därför att en generell utgångspunkt för när en ansiktsbild och de biometriska uppgifterna som tagits fram ur den bör uppdateras i ett identitetsindex är ett intervall om cirka tre till fem år. Detta bör säkerställa att de är riktiga och ändamålsenliga.

Begränsning till vissa ärenden och vissa myndigheter

Nästa fråga är vid vilka konkreta situationer som en uppdatering av ansiktsbild och biometriska uppgifter bör göras. En uppdatering av uppgifterna förutsätter att biometriska underlag har tagits upp. I kapitel 7 har vi redogjort för olika ärendeslag där biometriska underlag kan tas upp av Migrationsverket, Polismyndigheten och Skatteverket och i kapitel 13 har vi övervägt i vilka ärendeslag en identitetsnyckel bör kunna skapas. Som vi återkommer till i kapitel 18 och 21 bör biometriska underlag också få tas upp för att, genom en jämförelse mot ett identitetsindex, kunna verifiera identitet eller identifiera någon. Det skulle därför kunna övervägas att föreslå att ansiktsbilden och de biometriska uppgifter som kan tas fram ur den uppdateras vid varje sådant tillfälle. Vi anser emellertid att detta inte bör övervägas.

För det första skulle en sådan ordning medföra att uppdateringar riskerar att ske med en frekvens som inte är nödvändig, vilket belastar systemet och de myndigheter som uppdaterar uppgifterna. Det står inte heller i överensstämmelse med principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen. Vidare måste kvaliteten på de biometriska underlag som tas upp och därmed de uppgifter som

[6] *Ett säkert statligt ID-kort – med e-legitimation*, SOU 2019:14, s. 227.

ska ersätta de som finns lagrade i ett identitetsindex garanteras. Detta talar enligt vår mening tydligt för att begränsa vid vilka tillfällen dessa uppgifter bör kunna uppdateras. För det fall upptagningen inte är tillräckligt bra i ett visst fall när identiteten ska verifieras medför det eventuellt att verifieringen misslyckas. Nivån för när underlaget är tillräckligt bra för att genomföra en verifiering och när det är av tillräcklig kvalitet för att lagras som nytt jämförelsematerial i ett index kan dock antas skilja sig. I kapitel 21 bedömer vi att en bred krets av myndigheter bör få använda ett identitetsindex, bland annat genom biometrisk verifiering av identitet. Dessa aktörer har inte tillgång till samma tekniska utrustning eller samma erfarenhet av att bedöma kvalitet i biometriska underlag som de myndigheter som ansvarar för att etablera en grundidentitet, det vill säga Polismyndigheten, Migrationsverket och Skatteverket. Vi anser mot denna bakgrund att ansvaret för att uppdatera biometriska underlag och biometriska uppgifter i ett identitetsindex bör vila endast på sistnämnda myndigheter.

Det är som vi ser det inte heller lämpligt ur dataskyddshänseende att ge en relativt bred krets av myndigheter sådan tillgång till känsliga personuppgifter som behövs för att kunna uppdatera biometriska underlag och biometriska uppgifter (se kapitel 18 och 21 angående hur ett index bör kunna användas). I avsnitt 13.4.2 har vi bedömt att utlandsmyndigheterna inte bör kunna skapa en identitetsnyckel. De bör därför inte heller kunna uppdatera biometriska underlag och uppgifter i ett index.

Det ovan anförda begränsar de situationer när en uppdatering kan göras till Polismyndighetens, Migrationsverkets och Skatteverkets verksamhetsområden. Vi anser vidare att tidpunkten för när ansiktsbild och biometriska uppgifter ska uppdateras bör begränsas till vissa ärendeslag som dessa myndigheter handlägger, nämligen de där en identitetsnyckel – enligt våra bedömningar i kapitel 13 – hade kunnat skapas för en person som inte förekommer i ett identitetsindex. På detta sätt främjas effektivt att de uppgifter som ska användas för uppdateringen är av tillräcklig kvalitet och att de tagits upp i samma ordning som vid skapandet av en identitetsnyckel, vilket även kan ha tekniska fördelar. Vi anser därmed att ansiktsbild och biometriska uppgifter inte bör kunna uppdateras i ett index i andra situationer där biometriska underlag tas upp, exempelvis vid en gränskontroll. Vi hänvisar i denna del till de överväganden vi gjort i avsnitt 13.3.9.

Vi kan konstatera att de intervaller om cirka tre till fem år som vi nämnt ovan anknyter relativt väl till de giltighetstider som gäller för pass och för det statliga identitetskort som har föreslagits; giltighetstiderna för pass är – enligt 3 § andra stycket passlagen – fem år för personer som har fyllt tolv år och tre år för yngre personer. Det statliga identitetskortet föreslås få en giltighetstid om fem år, eller om sökanden inte har fyllt tolv år, tre år.[7] För de personkategorier som kan och ska kunna ansöka om nämnda handlingar kommer en uppdatering av ansiktsbild och biometriska uppgifter därmed att kunna göras inom intervall om tre till fem år. Det rör sig enligt vår bedömning om merparten av de personer som bör kunna omfattas av ett index. Om den enskilde väljer att vänta längre – exempelvis för att han eller hon under en längre tid inte har behov av pass – riskerar uppgifterna att förlora sin aktualitet. Det bör emellertid understrykas att detta inte automatiskt innebär att de inte är riktiga i den mening som avses i artikel 5.1 d i dataskyddsförordningen. De kan mycket väl återspegla de verkliga förhållandena trots att en längre tid har gått, särskilt för vuxna personer. Vi anser inte att det bör övervägas att föreslå någon skyldighet för den som är registrerad i ett identitetsindex att inleda ett ärende vid viss tidpunkt, endast i syfte att ge förutsättningar för att uppdatera ansiktsbilden och de biometriska uppgifterna. Det kan också ifrågasättas om det i praktiken alls finns ett behov av en sådan skyldighet, i vart fall för svenska medborgare. Detta med hänsyn till att innehav av pass eller en annan giltig identitetshandling får anses vara av central betydelse för att en individ överhuvudtaget ska kunna delta i det vardagliga livet i Sverige. Detta talar som vi ser det mycket starkt mot att en person medvetet skulle avstå från att ansöka om eller förnya ett pass eller en identitetshandling endast i syfte att ansiktsbilden och biometriska uppgifter i ett identitetsindex inte ska kunna uppdateras.

För personer som vistas i landet med ett tidsbegränsat uppehållstillstånd kan en uppdatering komma att ske med kortare intervall, beroende på tillståndets längd, i samband med att ett nytt uppehållstillståndskort utfärdas. För den med permanent uppehållstillstånd är giltighetstiden för uppehållstillståndskortet tre år, enligt bestämmelsen i 4 kap. 22 a § utlänningsförordningen (2006:97). Det innebär att ansiktsbilden och biometriska uppgifter även för personer som tillhör dessa personkategorier kan komma att uppdateras i ett identi-

[7] Promemorian *Ett statligt identitetskort*, Ju2026/01595, s. 68.

tetsindex med de intervaller som vi ovan har bedömt som lämpliga. Att uppdatering kan ske med kortare intervall för de som har tidsbegränsade uppehållstillstånd – i dag vanligtvis tretton månader eller två år – innebär enligt vår bedömning inte att uppgifterna behandlas i onödan på ett sätt som riskerar att hamna i konflikt med dataskyddsförordningen.

Vi kan här konstatera att för personer som vistas i Sverige med uppehållsrätt och som är registrerade i ett identitetsindex kan det antas att ansiktsbild och biometriska uppgifter inte kommer att uppdateras med samma intervall som för ovan nämnda personkategorier. De kan för det första inte få ett svenskt pass utfärdat och har ett mindre behov än svenska medborgare och tredjelandsmedborgare som är folkbokförda i landet av att ansöka om ett identitetskort som utfärdas av svenska myndigheter, eftersom de sannolikt har en godtagbar identitetshandling utfärdad av en annan medlemsstat. De har normalt sett inte heller uppehållstillstånd och därmed inte ett uppehållstillståndskort, som kan behöva förnyas. Vi anser visserligen att det kan vara en brist att ansiktsbild och biometriska uppgifter för personer som vistas i Sverige med stöd av uppehållsrätt inte kan antas komma att uppdateras med samma intervall som för övriga personkategorier. Det bör emellertid understrykas att endast den omständigheten att uppgifterna inte uppdateras med ett visst intervall inte behöver innebära att de har förlorat sin aktualitet och därmed inte längre är riktiga, utifrån det ändamål för vilket de behandlas. Vi anser därför att det saknas grund för att föreslå en särskild, separat ordning som endast syftar till att kunna uppdatera ansiktsbild och biometriska uppgifter för personer med uppehållsrätt. Med hänsyn till att uppehållsrätten dessutom kan upphöra utan något formligt beslut, och så att säga existerar vid varje given tidpunkt, kan det även medföra problem att bedöma om en viss person tillhör denna personkrets.

Ärenden om svenskt medborgarskap och ärenden i folkbokföringsverksamheten är inte av det slag att den enskilde kan antas inleda ett sådant ärende mer än vid ett eller enstaka tillfällen. Dessa ärenden kan därför generellt sett inte antas bidra till att uppgifter uppdateras med de regelbundna intervaller som vi förespråkar. Något som talar mot att ansiktsbilden och de biometriska uppgifterna ska kunna uppdateras även i de ärendeslagen, exempelvis vid en ändring av identitetsuppgift i folkbokföringen som föregås av en identitetskontroll och upptagning av biometriska underlag, har enligt vår bedömning dock

inte kommit fram. Även i dessa ärenden bör en uppdatering därför kunna ske.

Sammanfattning

Vi anser alltså att en ansiktsbild och biometriska uppgifter bör uppdateras av Polismyndigheten, Migrationsverket och Skatteverket när biometriska underlag tas upp i ett sådant ärende där en identitetsnyckel hade kunnat skapas (se kapitel 13). Vilken myndighet som kommer att vara ansvarig i det enskilda fallet beror på ärendeslaget. I likhet med uppdatering av identitetsuppgifter anser vi att en uppdatering *alltid* bör ske i ett identitetsindex när biometriska underlag tas upp i dessa situationer. Det ska alltså inte göras någon bedömning av om de biometriska underlagen och de uppgifter som tas fram ur dem i det enskilda fallet är ”bättre” än de som sedan tidigare behandlas i ett index. När det gäller ansiktsbild skulle det kräva en subjektiv bedömning av en handläggare. Det kan leda till informationskonflikter samt godtycklighet och osäkerhet i tillämpningen. Frågan om de biometriska underlagen är av tillräcklig kvalitet för att ersätta de redan lagrade får i stället avgöras av den programvara som används för att ta upp dem, och lösas på annat sätt än genom lagstiftning.

Med hänsyn till detta och till de intervall som vi anser att ansiktsbild och biometriska uppgifter bör kunna uppdateras med bedömer vi att dessa uppgifter, vid ett givet tillfälle då en verifiering eller en identifiering kan komma att göras mot ett identitetsindex, kommer att återspegla de verkliga förhållandena och därmed vara riktiga på det sätt som avses i artikel 5.1 d i dataskyddsförordningen.

14.3.7 Kontroller när en uppgift ska uppdateras

När en uppgift i ett identitetsindex uppdateras i syfte att den ska vara aktuell, i de situationer som vi redogjort för i avsnitt 14.3.2–14.3.6, måste den myndighet som gör uppdateringen förvissa sig om att uppdateringen görs för rätt individ. I annat fall kommer uppgiften inte att vara riktig i den mening som avses i artikel 5.1 d i dataskyddsförordningen. Tillförlitligheten till ett index riskerar även att snabbt påverkas negativt. Rätt individ måste alltså lokaliseras i indexet. I de situationer som beskrivits i avsnitt 14.3.2–14.3.6 får en jämförelse

ske mellan de uppgifter som är knutna till en viss identitetsnyckel och andra uppgifter som är tillgängliga i det enskilda fallet, det vill säga en verifiering av identiteten. Det är emellertid inte fråga om att i första hand få svar på frågan *Är en viss person den som han eller hon utger sig för att vara?* utan verifieringen syftar i dessa situationer till att kontrollera att rätt individ (identitetsnyckel) har lokaliserats. Det innebär att en verifiering inte, endast, kan ske genom att jämföra uppgifter i en identitetshandling som den enskilde överlämnar med underlag som har tagits upp från innehavaren, utan en kontroll behöver göras mot identitetsindexet. Hur kontrollen sker beror på omständigheterna i det enskilda fallet.

Om biometriska underlag har tagits upp – exempelvis vid en ansökan om pass eller medborgarskap – bör biometrisk verifiering mot identitetsindexet användas i första hand, eftersom tillförlitligheten i en sådan verifiering är mycket hög; genom att en biometrisk verifiering görs kan det enligt vår bedömning i princip uteslutas att uppgifter uppdateras för en annan individ än den som är aktuell i det ärende som föranlett att en uppgift behöver uppdateras. Om biometriska underlag däremot inte är tillgängliga får verifieringen ske på annat sätt. Om exempelvis en uppgift om identiteten behöver uppdateras av Skatteverket som en följd av att någon har bytt efternamn (se avsnitt 14.3.2), kan verifieringen i praktiken gå till så att en identitetsnyckel lokaliseras i ett identitetsindex med hjälp av personnumret för den enskilde, varefter en jämförelse görs mellan de identitetsuppgifter som är kopplade till den individ som på detta sätt har lokaliserats och de som finns i folkbokföringen och i ärendet. Om en ansiktsbild finns tillgänglig för myndigheten, exempelvis i Migrationsverkets dossier i samband med att födelsetid för en person ändras i centrala utlänningsdatabasen, kan denna jämföras med den som finns lagrad i ett identitetsindex, för att främja tillförlitligheten i kontrollen.

Eftersom ett identitetsindex, enligt våra överväganden i kapitel 21, bör kunna användas för att verifiera identitet med grund i biometriska uppgifter i många fler situationer än vad som är möjligt i dag skulle det kunna övervägas en skyldighet att lämna biometriska underlag i syfte att verifiera identiteten i *samtliga* situationer då uppgifter i ett identitetsindex behöver uppdateras på det sätt som framgår av avsnitt 14.3.2–14.3.6. En sådan skyldighet skulle emellertid kunna utgöra ett oproportionerligt intrång i rätten till skydd för privatlivet

enligt artikel 8.1 i Europeiska konventionen om skydd för de mänskliga rättigheterna, Europakonventionen. Detta skydd inbegriper i vissa fall en rätt till skydd mot att bli fotograferad. Vidare skulle ett generellt krav om att lämna biometriska underlag kunna innebära ett krav även på att personen inställer sig personligen, vilket kan upplevas som praktiskt betungande för både den enskilde och myndigheten i fråga. Vid en sammantagen bedömning anser vi att det inte generellt bör krävas att biometrisk verifiering används för att lokalisera rätt identitetsnyckel i ett identitetsindex, när en uppgift ska uppdateras i syfte att bibehålla dess aktualitet.

Det ovan anförda kan ge intryck av att det kan vara problematiskt för en myndighet att förvissa sig om att rätt individs uppgifter uppdateras i de situationer som framgår av avsnitt 14.3.2–14.3.6. Vår bedömning är att så normalt sett inte är fallet. Det kan med fog antas att myndigheten har vidtagit nödvändiga utredningsåtgärder för att kontrollera identiteten på individen i det ärende som föranleder att en viss uppgift i ett identitetsindex behöver uppdateras. I samband med detta bör det även finnas möjlighet att ta fram andra relevanta uppgifter som identitetsbeteckning och identitetsnyckel. Redan i detta skede kan en verifiering mot indexet alltså ha gjorts, med tillämpning av någon av de metoder som vi redogjort för ovan. Huruvida rätt individ har lokaliserats ankommer på den myndighet som ska uppdatera en uppgift att ta ställning till. Nedan beskrivs några typsituationer.

1. Migrationsverket anser att födelsetid för en viss individ som har ansökt om uppehållstillstånd behöver uppdateras, efter att ny information har kommit fram. Individnumret som sökanden har tilldelats är känt för myndigheten och det kan användas för att lokalisera individen i ett identitetsindex. Uppgift om personens identitetsnyckel kan också finnas i den dossier som finns upplagd för honom eller henne hos Migrationsverket. En jämförelse av ansiktsbilden som är lagrad för individen kan därefter göras mot den som finns i Migrationsverkets dossier. I detta sammanhang kan vi även notera att förslag har lämnats i regeringens proposition S*tärkt återvändandeverksamhet* om att Migrationsverket, vid en muntlig utredning av rätten till uppehållstillstånd, ska få ta upp biometriska underlag om identiteten inte kan klarläggas på annat

sätt.[8] I så fall kan en biometrisk verifiering mot identitetsindexet göras i sådana situationer.

2. Skatteverket ändrar uppgift om namn i folkbokföringsverksamheten och denna uppgift ska därför uppdateras även i ett identitetsindex. Det kan antas att myndigheten har utrett vilken person som ändringen i folkbokföringen avser och därmed även har tillgång till dennes person- eller samordningsnummer. Identitetsbeteckningen kan användas för att lokalisera individen i ett index. En jämförelse kan då göras mellan de identitetsuppgifterna som är kopplade till individen och de som finns i ärendet, vilken utgör den påstådda identiteten, för att verifiera identiteten. Om en identitetskontroll enligt bestämmelserna i 26 a–c §§ folkbokföringslagen har föregått ändringen av identitetsuppgifter kan en biometrisk verifiering också användas.
3. En ansiktsbild behöver uppdateras vid en ansökan om pass hos Polismyndigheten. Den ansiktsbild som tagits upp med stöd av 6 § passlagen och de biometriska uppgifter som kan tas fram ur den kan då användas för att verifiera identitet mot ett index, efter att individen lokaliserats, antingen med hjälp av en identitetsnyckel eller genom en sökning med personnummer.
4. Migrationsverket bedömer i samband med en ansökan om förnyelse av ett uppehållstillståndskort att födelsetiden för sökanden ska ändras i den centrala utlänningsdatabasen, och därmed även i ett index. En biometrisk verifiering kan då göras med hjälp av underlag som har tagits upp med stöd av 9 kap. 8 a § utlänningslagen (2005:716). Lokaliseringen av individen i ett identitetsindex kan göras med individnummer, eventuell identitetsbeteckning eller en identitetsnyckel.

14.4 Rättelse och radering av felaktiga uppgifter

Genom våra överväganden i avsnitt 14.3.2–14.3.6 bedömer vi att uppgifterna i ett identitetsindex för en viss individ kommer att kunna uppdateras i den utsträckning som krävs för att de – normalt sett – ska anses riktiga enligt artikel 5.1 d i dataskyddsförordningen. Det

[8] Prop. 2025/26:263, s. 135. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.

kan dock tänkas att felaktigheter uppstår som inte kan hänföras till att uppgifterna inte är aktuella.

En felaktig uppgift kan tänkas uppkomma till följd av en myndighets eller någon annans skrivfel, räknefel eller något annat liknande förbiseende. Det skulle kunna röra sig om att det vid ändring av ett efternamn i folkbokföringen, i ett senare skede, upptäcks av Skatteverket att två bokstäver i det nya namnet av misstag har kastats om i den namnuppgift som registrerades i ett index, men att uppgifterna i folkbokföringsverksamheten är korrekta. När det gäller ansiktsbild och biometriska uppgifter kan det ifrågasättas om felaktigheter alls kan uppstå i ett identitetsindex för sådana uppgifter. Detta eftersom de ska kunna knytas till en identitetsnyckel endast inom ramen för de ärendeslag som vi redogjort för i kapitel 13. Det framstår enligt vår bedömning som mycket osannolikt att det inte skulle uppmärksammas att uppgifter registreras för fel person i ett sådant ärende; vid exempelvis en passansökan skulle felaktigheten innebära att en passhandling innehåller fel foto eller biometriska underlag, vilket får anses som i princip uteslutet, med hänsyn till de kontroller som sker i ett sådant ärende. Tekniska fel kan emellertid tänkas resultera i att biometriska uppgifter korrumperas i databasen och därmed inte längre överensstämmer med de verkliga förhållandena. I detta avsnitt belyser vi hur *felaktiga* uppgifter i ett identitetsindex bör kunna rättas och, i vissa fall, raderas.

I detta sammanhang kan vi konstatera att en allmän möjlighet till rättelse följer av 36 § förvaltningslagen. Bestämmelsen ger stöd för en myndighet att rätta uppenbara felaktigheter i ett beslut som myndigheten fattat. En rättelse av en uppgift i ett identitetsindex kan som vi ser det dock inte göras med stöd av bestämmelsen. För det första kan en registrering eller uppdatering av uppgifter i ett identitetsindex inte naturligt sägas göras genom ett beslut. I vart fall kommer det inte att manifesteras i någon särskild beslutshandling. En felaktig uppgift kan dessutom tänkas uppstå på grund av ett tekniskt fel, vilket inte omfattas av nyss nämnda bestämmelse. Den möjlighet till rättelse som följer av bestämmelsen i 36 § förvaltningslagen täcker därför inte behovet av att kunna rätta felaktigheter som uppkommit på detta sätt. Bestämmelsen är dessutom begränsad på så sätt att felaktigheten ska vara uppenbar. Den skyldighet att se till att personuppgifter som behandlas är riktiga som följer av artikel 5.1 d i dataskyddsförordningen innehåller inte någon motsvarande begräns-

ning. En felaktig uppgift i ett index måste enligt vår mening kunna uppdateras oavsett anledningen till att felaktigheten har uppstått, och bör inte heller begränsas på så sätt att uppdateringen endast kan ske på initiativ av en myndighet.

14.4.1 Rättelse och radering enligt dataskyddsförordningen

Vår bedömning

En felaktig uppgift i ett identitetsindex bör genom en rättelse enligt dataskyddsförordningen uppdateras även i andra situationer än de som anges i avsnitt 14.3.2–14.3.6. Rätten till rättelse bör inte inskränkas. Om det saknas en korrekt uppgift ska den felaktiga uppgiften raderas.

Oavsett anledningen till att en viss uppgift i ett identitetsindex är felaktig anser vi att den utan dröjsmål bör uppdateras genom att den rättas eller, under vissa förutsättningar, raderas. Det är naturligtvis inte ändamålsenligt att en objektivt konstaterbar felaktig uppgift inte kan uppdateras annat än i de situationer som vi redogjort för i avsnitt 14.3. Att den enskilde skulle vara tvungen att exempelvis ansöka om ett pass endast för att kunna rätta en felaktig uppgift är som vi ser det inte rimligt; ett sådant ärende är dessutom förenat med en ansökningsavgift. Att den personuppgiftsansvarige har en skyldighet att på eget initiativ vidta sådana åtgärder följer direkt av artikel 5.1 d i dataskyddsförordningen. Den registrerade har även en möjlighet enligt artikel 16 i dataskyddsförordningen att, av den personuppgiftsansvarige, utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Bestämmelsen ska tolkas mot bakgrund av artikel 5.1 d men även mot bakgrund av skäl 59 i förordningen, enligt vilket förfaranden bör fastställas som gör det lättare för registrerade att utöva sina rättigheter enligt förordningen, inklusive mekanismer för att begära och i förekommande fall få tillgång till och bland annat erhålla rättelse av personuppgifter. Bestämmelserna om rättelse motiveras av integritetsskäl.[9]

[9] *Författningsändringar på finansmarknadsområdet med anledning av EU:s dataskyddsförordning*, prop. 2017/18:142, s. 48.

Av artikel 23 i dataskyddsförordningen följer att rätten till rättelse kan begränsas i nationell rätt om en sådan begränsning sker med respekt för andemeningen i de grundläggande fri- och rättigheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att säkerställa vissa i artikeln angivna syften. Ett sådant syfte är andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse (artikel 23.1 e). Ett annat syfte är skydd av den registrerade eller andras rättigheter och friheter (artikel 23.1 i).

Rätten till rättelse utgör enligt vår mening inte något hinder för att ett identitetsindex ska kunna fungera på ett ändamålsenligt sätt. Detta inte minst med hänsyn till att ett sådant systems funktion och effektivitet till stor del är avhängig av att de uppgifter som behandlas i det är riktiga. Även om ett identitetsindex syftar till att på ett effektivt sätt kunna motverka identitetsmissbruk – vilket enligt våra överväganden i avsnitt 16.4.3 är ett viktigt allmänt intresse – anser vi därför att det saknas anledning att med hänsyn till detta inskränka rätten till rättelse enligt artikel 16 i dataskyddsförordningen.

Endast objektivt felaktiga uppgifter omfattas

En rättelse med stöd av dataskyddsförordningen förutsätter att uppgiften i fråga är felaktig och att den kan ersättas med en korrekt uppgift. Med att en uppgift är felaktig menas att den, utifrån ändamålet för behandlingen av den, inte stämmer med verkliga förhållanden. Rättelse används i första hand när det är enkelt för den personuppgiftsansvarige att objektivt avgöra om det föreligger en felaktig behandling av en personuppgift, till exempel genom att fel personnummer har angetts för en individ. I en sådan situation bör det sällan råda någon oenighet i fråga om uppgiften är felaktig eller inte. Om det däremot krävs en mer ingående materiell prövning ska rättelsen inte ske enligt dataskyddsförordningen. Det är inte möjligt att närmare ange när en uppgift i ett identitetsindex ska anses felaktig i ett enskilt fall utan det ankommer på den som ska rätta uppgiften att ta ställning till om den är felaktig. Vissa övergripande observationer kan emellertid lyftas fram.

När det gäller de alfanumeriska uppgifter som bör få behandlas – det vill säga identitetsuppgifter, en identitetsbeteckning eller Migrationsverkets individnummer – har vi i avsnitt 14.3 bedömt att dessa

är riktiga om de överensstämmer med motsvarande uppgifter i folkbokföringsverksamheten eller den centrala utlänningsdatabasen, för en viss individ. Att avgöra om en uppgift av sådant slag är objektivt felaktig bör därmed i normalfallet inte vålla några problem utan innefattar att en jämförelse görs mellan uppgifterna i de olika registren. I en sådan situation torde det sällan råda oenighet om uppgiften är felaktig eller inte. Jämförelsen förutsätter emellertid att det går att lokalisera rätt individ i respektive register; i annat fall går det inte att veta att rätt underlag jämförs. För att lokalisera individen i ett index kan identiteten behöva verifieras på något av de sätt som vi beskrivit i avsnitt 14.3.7, eller på annat sätt som den personuppgiftsansvarige anser är lämpligt. Om en felaktig uppgift upptäcks av den myndighet som också, enligt våra förslag nedan, ska rätta uppgiften, bör några problem med att lokalisera rätt individ givetvis inte uppstå; det är då, genom att felaktigheten i sig har upptäckts, utrett vilken individ som den felaktiga uppgiften är kopplad till.

Att en ansiktsbild eller en biometrisk uppgift i ett identitetsindex är felaktig innebär, utifrån våra överväganden i avsnitt 14.3.6, att de inte återspeglar de fysiska kännetecken som individen har vid ett givet tillfälle. I vissa fall kan det vara enkelt att konstatera. Om till exempel ansiktsbilden i ett index har gått förlorad eller har blivit helt svart, på grund av tekniska problem, är den enligt vår mening alltid att betrakta som objektivt felaktig. Att den registrerade eller en handläggare vid en myndighet anser att ansiktsbilden inte är särskilt välliknande eller smickrande, eller anser att det finns en annan bild med bättre skärpa eller ljusförhållanden, innebär enligt vår mening däremot inte att uppgiften bör ses som felaktig.

För att avgöra om en biometrisk uppgift är felaktig bör normalt krävas att en datorstödd jämförelse görs, om det inte på ett enkelt sätt går att konstatera att informationen i indexet har korrumperats eller raderats; om det helt saknas biometriska uppgifter för en viss individ är uppgiften att betrakta som felaktig, eftersom den då per definition inte kan motsvara de verkliga förhållandena. Att en biometrisk verifiering inte lyckas behöver däremot inte betyda att en uppgift i ett identitetsindex är felaktig utan det kan bero på andra faktorer. Exempelvis kan upptagningen av de biometriska underlagen i samband med verifieringen brista i ett visst fall på grund av tekniska problem med utrustningen. Det kan även vara så att den individ som lämnar de biometriska underlagen inte är den person som han eller

hon utger sig för att vara och att de biometriska uppgifterna som tas fram ur underlagen därför inte avser den individ som rättelsen avser. Sammantaget får bedömningen av om de biometriska uppgifterna är objektivt felaktiga i den mening som avses i dataskyddsförordningen avgöras av den som har att rätta dem, utifrån omständigheterna i det enskilda fallet. Om det inte går att på ett enkelt sätt konstatera att information exempelvis helt saknas eller har korrumperats, eller tillhör en annan individ, krävs som vi ser det sannolikt att bedömningen av om uppgiften är felaktig görs med stöd av den programvara som används för den biometriska jämförelsen, utifrån hur högt matchningsresultat jämförelsen generar.

En rättelse förutsätter att det finns korrekta uppgifter

För det fall det går att konstatera att en alfanumerisk uppgift i ett identitetsindex är objektivt felaktig bör den rättas med de uppgifter som finns i folkbokföringsverksamheten eller den centrala utlänningsdatabasen; dessa uppgifter utgör – i enlighet med våra överväganden i avsnitt 14.3.2–14.3.5 – de korrekta (riktiga) uppgifterna. Det går däremot inte att rätta sådana uppgifter i ett index direkt genom att exempelvis komma in med en ny identitetshandling, eftersom uppgifterna i handlingen inte utgör de verkliga förhållanden som uppgifterna ska återspegla; i sådana fall får den enskilde begära att uppgifterna i folkbokföringsverksamheten eller den centrala utlänningsdatabasen ändras. Något kompletterande underlag från den registrerade är därför inte heller av betydelse i de fall en alfanumerisk uppgift i ett identitetsindex behöver rättas.

Situationen är en annan om ansiktsbild eller biometriska uppgifter i ett index behöver rättas. Korrekta uppgifter är i sådana fall inte alltid tillgängliga på samma sätt som när en alfanumerisk uppgift rättas. Om exempelvis Skatteverket upptäcker att ett tekniskt fel har lett till att en ansiktsbild i ett identitetsindex har raderats behöver ett nytt sådant underlag vara tillgängligt. Det kan tänkas att det på teknisk väg är möjligt att få fram ett underlag – exempelvis genom en säkerhetskopia – men det kan i många fall krävas att den registrerade vars uppgifter är felaktiga lämnar biometriska underlag som kan användas för att rätta en felaktig ansiktsbild eller biometrisk uppgift. Detta får enligt vår bedömning lösas med utgångspunkt i de normala utred-

ningsåtgärder som en myndighet kan vidta i ett ärende. Det kan i vissa fall innebära att en felaktig ansiktsbild eller felaktiga biometriska uppgifter inte kan rättas. Vi anser dock inte att det bör finnas någon skyldighet för den enskilde att lämna biometriska underlag endast i syfte att en uppgift ska kunna rättas. Som skäl för denna bedömning hänvisar vi till vad vi anfört i avsnitt 14.3.7 angående att det inte generellt bör krävas att biometrisk verifiering används när en uppgift uppdateras i syfte att bibehålla dess aktualitet.

Om en felaktig uppgift inte kan rättas ska den raderas

Med hänsyn till att det för alfanumeriska uppgifter alltid kommer att finnas uppgifter som är riktiga tillgängliga – nämligen de som finns registrerade i folkbokföringsverksamheten eller den centrala utlänningsdatabasen – för den individ vars uppgifter behöver rättas i ett identitetsindex kommer det som vi ser det inte att i något fall bli aktuellt att radera sådana uppgifter.

När det gäller ansiktsbild eller biometriska uppgifter kan en rättelse av dessa däremot förutsätta medverkan från den enskilde, genom att han eller hon lämnar biometriska underlag. Om det i ett enskilt fall av någon anledning inte är möjligt att få fram uppgifter som kan användas för en rättelse, exempelvis med hänsyn till att den enskilde inte kan, eller vill, lämna biometriska underlag i syfte att uppgifterna ska kunna uppdateras, följer det av artikel 5.1 d i dataskyddsförordningen att den felaktiga uppgiften ska raderas. Redan med hänsyn till utformningen av nämnda bestämmelse anser vi att det saknas utrymme för att fortsätta behandla en felaktig uppgift i ett identitetsindex, för att den inte går att rätta. Sett till syftet med ett identitetsindex kommer en radering av biometriska uppgifter för en individ att innebära att hans eller hennes identitet inte går att verifiera biometriskt mot systemet. Detta framstår, mot bakgrund av att syftet med ett index är just att biometriska uppgifter ska kunna användas för verifiering i större utsträckning, givetvis som en mindre ändamålsenlig ordning. Vi kan dock konstatera att en sådan begränsning inträder redan när uppgiften är att betrakta som felaktig; en verifiering går inte att göra mot felaktiga biometriska uppgifter. Raderingen i sig medför alltså inte någon ytterligare begränsning. Det saknas vidare, som vi ser det, hinder mot att biometriska upp-

gifter uppdateras, genom att nya registreras för individen i fråga, vid ett senare tillfälle, inom ramen för något sådant ärende som vi beskrivit i avsnitt 14.3.6. Vi kan också konstatera att ett syfte med ett identitetsindex är att den enskilde ska kunna känna sig trygg med att andra inte kan uppträda som honom eller henne, genom möjligheten till biometrisk verifiering i olika sammanhang. Det kan därför finnas ett incitament för den enskilde att medverka till att lämna biometriska underlag så att en felaktig uppgift kan rättas eller, i annat fall, ta initiativ till att de uppdateras vid ett senare tillfälle.

Med hänsyn till detta och till att det framstår som osannolikt att biometriska uppgifter överhuvudtaget skulle kunna bli felaktiga (se inledningen till avsnitt 14.4) annat än genom ett tekniskt fel, bör radering av sådana uppgifter i praktiken endast behöva göras i absoluta undantagsfall.

14.4.2 Ansvar för att rätta eller radera en felaktig uppgift

Vår bedömning

En uppdatering av en alfanumerisk uppgift i ett identitetsindex genom att den rättas eller raderas enligt dataskyddsförordningen bör för personer som har en identitetsbeteckning göras av Skatteverket och i annat fall av Migrationsverket. En ansiktsbild och biometriska uppgifter bör rättas eller raderas av Polismyndigheten, Migrationsverket eller Skatteverket.

Frågan är vem som bör kunna uppdatera en felaktig uppgift genom att rätta eller radera den. Den krets av aktörer som kan tänkas upptäcka att ett identitetsindex innehåller en uppgift som är felaktig kan omfatta andra än Polismyndigheten, Migrationsverket och Skatteverket (se kapitel 21 om olika aktörers användning av ett index). Det är inte heller osannolikt att den registrerade själv är den som upptäcker en felaktighet och då begär rättelse enligt dataskyddsförordningen. Vi anser emellertid att endast nyss nämnda myndigheter bör kunna rätta eller radera en felaktig uppgift i ett index. En annan ordning skulle vara svår att förena med våra överväganden i avsnitt 14.3.2–14.3.6. Det är enligt vår bedömning lämpligast att en felaktig uppgift rättas eller raderas av den myndighet som, enligt nämnda avsnitt,

ansvarar för att i normala fall uppdatera den typ av uppgift som det är fråga om. Detta inte minst eftersom en felaktighet som uppstår av misstag ofta kan tänkas uppstå i samband med att en uppgift registreras eller uppdateras av myndigheten i fråga av annan anledning. Denna myndighet har då sannolikt lättast att rätta en uppgift, då den så att säga har ”närmst” till en korrekt uppgift som kan användas för att uppdatera en felaktig uppgift. Att en viss myndighet har en stor närvaro i samhället kan också vara en faktor att beaktas.

Alfanumeriska uppgifter

När det gäller identitetsuppgifter, person- och samordningsnummer samt Migrationsverkets individnummer har vi i avsnitt 14.3.2–14.3.5 föreslagit att Skatteverket respektive Migrationsverket bör ansvara för att uppdatera dessa uppgifter, beroende på typen av uppgift och personkategori i det enskilda fallet. Något som talar mot att ansvaret bör fördelas på samma sätt vid uppdatering i form av en rättelse eller radering av en felaktig uppgift av detta slag har enligt vår bedömning inte kommit fram. Skatteverket och Migrationsverket har inom ramen för sina verksamheter tillgång till de korrekta uppgifterna i folkbokföringsverksamheteten respektive den centrala utlänningsdatabasen och bör därmed förhållandevis enkelt kunna rätta en felaktig uppgift. Att samma myndighet ansvarar för uppdateringen av dessa uppgifter – oavsett orsak – har enligt vår mening tydliga fördelar, bland annat genom att man kan dra nytta av befintliga resurser och beslutsstöd samt tekniska system. Vi anser alltså att en uppdatering i form av en rättelse eller radering av en alfanumerisk uppgift i ett identitetsindex bör göras av Skatteverket för den som har en identitetsbeteckning och i annat fall av Migrationsverket.

Ansiktsbilder och biometriska uppgifter

Beträffande ansiktsbilder och biometriska uppgifter har vi i avsnitt 14.3.6 bedömt att en uppdatering bör göras av Polismyndigheten, Migrationsverket eller Skatteverket, beroende på vem av dessa myndigheter som handlägger det ärende som föranleder uppdateringen. En rättelse eller radering för att en uppgift är felaktig kan emellertid behöva göras utan samband med ett sådant ärende. Det är därför

inte möjligt att peka ut en ansvarig myndighet på samma sätt som vid en uppdatering som sker för att en uppgift ska vara aktuell. Samtidigt innebär det som vi ser det att det saknas hinder mot att göra en annan bedömning i fråga om vem som ska rätta en felaktig ansiktsbild eller biometrisk uppgift. För att sådana uppgifter ska kunna rättas kan det också vara en förutsättning att den enskilde medverkar genom att lämna biometriska underlag. Organisatoriska faktorer som tillgång till utrustning för att ta upp sådana underlag eller särskild kompetens i identitetsfrågor bör därför också beaktas.

I avsnitt 13.4.1 har vi bedömt att Polismyndigheten, Migrationsverket och Skatteverket – beroende på ärendeslag – bör kunna skapa en identitetsnyckel. I samband med det tas biometriska underlag upp och olika kontroller görs av identiteten. Med hänsyn till detta anser vi att dessa myndigheter som utgångspunkt också får anses ha tillgång till nödvändig organisation, kompetens och utrustning för att på ett tillförlitligt sätt kunna rätta en felaktig ansiktsbild eller biometrisk uppgift. Det kan, som vi ser det, dock finnas skillnader mellan myndigheterna i sådana avseenden, som skulle kunna tala för att fördela ansvaret för att rätta eller radera en felaktig uppgift på annat sätt än enligt våra bedömningar i avsnitt 13.4.1 och 14.3.

Ansvaret bör inte samlas hos en myndighet

Att samla ansvaret hos en enda myndighet skulle kunna främja en tydlighet i ansvarsfördelningen, men också underlätta för den enskilde, genom att det blir enklare för den som vill begära rättelse att veta var han eller hon ska vända sig. Den ökade arbetsbörda som rättelse av en ansiktsbild och en biometrisk uppgift kan tänkas medföra är enligt vår mening inte ett tungt vägande skäl mot att samla ansvaret hos en myndighet, med hänsyn till att vi i avsnitt 14.4.1 bedömt att felaktigheter avseende sådana uppgifter mycket sällan kan antas uppkomma.

För det fall ansvaret bör samlas hos en myndighet bör Polismyndigheten i första hand övervägas. För det första kan vi konstatera att myndigheten kommer att vara den som möter majoriteten av de som kan komma att omfattas av ett identitetsindex, nämligen svenska medborgare. I avsnitt 13.4.1 har vi redogjort för omständigheter som talar för att samla ansvaret för att skapa en identitetsnyckel

hos Polismyndigheten, bland annat myndighetens större närvaro i samhället samt erfarenhet av identitetskontroller och av att ta upp biometriska underlag i samband med detta. Dessa omständigheter bör beaktas även i detta sammanhang. Vidare kan konstateras att Utredningen om säker och tillgänglig digital identitet lyfte fram det faktum att Polismyndigheten har huvudsakligt ansvar för att motverka identitetsrelaterad brottslighet, som en omständighet som med styrka ansågs tala för att denna myndighet bör ansvara för grundidentifieringen vid utfärdande av en sådan statlig e-legitimation som föreslogs av utredningen. Utöver dessa organisatoriska och kompetensrelaterade faktorer pekades på att en inställelse hos Polismyndigheten i sig har en brottsavhållande funktion eftersom det är mindre sannolikt att någon presenterar en förfalskad id-handling för en polistjänsteman än för en handläggare på Skatteverket.[10]

Det finns dock omständigheter som talar i motsatt riktning. För det första kan felaktigheter i fråga om en ansiktsbild eller biometriska uppgifter uppstå i samband med att uppgifterna antingen registreras när en identitetsnyckel skapas eller när de uppdateras i enlighet med våra överväganden i avsnitt 14.3. Det är då viktigt att de snabbt kan rättas. Det framstår som givet att det i en sådan situation är den myndighet – exempelvis Skatteverket i ett ärende om flyttning till Sverige – som orsakade felaktigheten som snabbast och enklast kan rätta uppgiften. I annat fall skulle den enskilde eventuellt tvingas att lämna nya biometriska underlag hos Polismyndigheten, vid ett separat tillfälle och på annan plats. Redan risken för sådana konsekvenser talar enligt vår mening mycket starkt mot att samla ansvaret hos sistnämnda myndighet. Även i de fall då en felaktig uppgift upptäcks i efterhand är det inte osannolikt att den myndighet som registrerat en identitetsnyckel och eventuellt tidigare har uppdaterat en ansiktsbild och biometriska uppgifter för en viss individ har tillgång till korrekta uppgifter som kan användas för att rätta felaktigheten, och då utan den enskildes medverkan. Om den registrerade vill begära rättelse kan det också antas vara naturligt att han eller hon i första hand kontaktar den myndighet som han eller hon senast hade kontakt med i ett sådant ärende.

Det finns alltså omständigheter som talar både för och emot att samla ansvaret för att rätta eller radera felaktiga uppgifter i form av en ansiktsbild och biometriska uppgifter hos en enda myndighet,

[10] *En säker och tillgänglig statlig e-legitimation*, SOU 2023:61, s. 177 f.

företrädesvis Polismyndigheten. De omständigheter som talar för är emellertid som vi ser det framför allt hänförliga till en större erfarenhet av identitetskontroller, men även tillgång till fler platser där biometriska underlag kan tas upp. Sett i ljuset av att vi bedömer att rättelse av ansiktsbilder och biometriska uppgifter kan antas behöva göras i mycket få fall kan sistnämnda faktor inte anses avgörande. Beträffande erfarenhet och kompetens bedömer vi att en rättelse eller radering av sådana uppgifter normalt inte innefattar större krav på särskild kompetens än vad som förutsätts vid skapandet av en identitetsnyckel. De brottsförebyggande effekter som en inställelse hos Polismyndigheten i andra sammanhang har bedömts föra med sig är enligt vår bedömning inte heller något tungt vägande skäl i det aktuella sammanhanget. I stället anser vi att de omständigheter som lyfts fram i föregående stycke i fråga om tillgång till korrekta uppgifter och ett behov av att snabbt och enkelt kunna rätta en uppgift talar starkt för att ansvaret inte bör samlas hos en enda myndighet.

Rättelse eller radering bör kunna göras av alla tre myndigheter

Frågan är om ansvaret bör fördelas på något särskilt sätt mellan Polismyndigheten, Migrationsverket och Skatteverket. Som vi konstaterat ovan är det inte möjligt att utgå från ärendeslaget. Det kan däremot övervägas att fördela ansvaret utifrån personkategori, på liknande sätt som vi föreslår avseende alfanumeriska uppgifter. En utgångspunkt skulle kunna vara en fördelning som utgår från följande personkategorier: svenska medborgare, EES-medborgare, tredjelandsmedborgare med identitetsbeteckning och tredjelandsmedborgare som saknar en identitetsbeteckning. Att avgöra vilken kategori som en viss individ tillhör kan i normalfallet inte antas vålla några svårigheter, varken för den enskilde eller för den myndighet som har att ta ställning till om uppgiften ska rättas eller raderas. En ansiktsbild och biometriska uppgifter bör, enligt vad vi anfört i avsnitt 13.3 och 14.3, kunna registreras i ett index vid skapandet av en identitetsnyckel samt uppdateras löpande på följande sätt.

Tabell 14.2 Ansvar för registrering och uppdatering för olika personkategorier

Personkategori	Registreras eller uppdateras i ett ärende om	Av
Svenska medborgare	Pass eller statligt identitetskort	Polismyndigheten
	Statlig e-legitimation	-"-
	Flyttning till Sverige	Skatteverket
	Ändring i folkbokföringen	-"-
EES-medborgare	Flyttning till Sverige	Skatteverket
	Samordningsnummer	-"-
	Ändring i folkbokföringen	-"-
	Statligt identitetskort	Polismyndigheten
	Statlig e-legitimation	-"-
Tredjelandsmedborgare med identitetsbeteckning	Flyttning till Sverige	Skatteverket
	Samordningsnummer	-"-
	Ändring i folkbokföringen	-"-
	Statligt identitetskort	Polismyndigheten
	Statlig e-legitimation	-"-
	Svenskt medborgarskap	Migrationsverket
Tredjelandsmedborgare utan identitetsbeteckning	Uppehållstillstånd	Migrationsverket
	Uppehållstillståndskort	-"-

Utifrån den ovanstående uppställningen kan några övergripande observationer göras. Det kan på goda grunder antas att svenska medborgare, i den stora majoriteten av situationer, har kontakt med bara Polismyndigheten i ärenden som föranleder att en ansiktsbild och biometriska uppgifter registreras eller uppdateras i ett identitetsindex; en svensk medborgare kommer inte att ha kontakt med Migrationsverket i ett sådant ärende som avses i avsnitt 13.3 och 14.3 och med Skatteverket endast i relativt få relevanta fall. Ett undantag som kan noteras är utländska medborgare som naturaliserats och blivit svenska medborgare – i dessa fall kommer personen i fråga tidigare att ha haft kontakt med både Migrationsverket och Skatteverket. Antalet ärenden om naturalisation är enligt vår bedömning dock – jämfört med antalet ärenden om pass och identitetskort – relativt få. Tredjelandsmedborgare som saknar identitetsbeckning kommer, så länge han eller hon tillhör den personkategorin, att kunna registreras i ett identitetsindex eller få uppgifter i ett sådant register uppdaterade, i enlighet med våra överväganden i avsnitt 14.3, endast av Migrationsverket. För såväl EES-medborgare som tredjelandsmedborgare som har en identitetsbeteckning kan ansvaret för regi-

strering respektive uppdatering av uppgifter i syfte att de ska vara aktuella däremot variera över tid, på ett annat sätt än för ovan nämna personkategorier. Exempelvis kan en identitetsnyckel skapas av Migrationsverket när ett uppehållstillståndskort utfärdas, varefter uppgifterna uppdateras av Skatteverket när utlänningen anmäler flyttning till Sverige. Om ett nytt uppehållstillståndskort utfärdas för personen under vistelsen i landet eller personen beviljas svenskt medborgarskap är det i stället Migrationsverket – enligt våra överväganden i avsnitt 14.3.6 – som bör uppdatera ansiktsbilden och de biometriska uppgifterna. Om personen dessutom får ett sådant statligt identitetskort utan resefunktion som har föreslagits i promemorian *Ett statligt identitetskort* utfärdat kommer ansiktsbilden och de biometriska uppgifterna att uppdateras av Polismyndigheten.

För svenska medborgare och tredjelandsmedborgare som saknar identitetsbeteckning skulle visserligen Polismyndigheten respektive Migrationsverket kunna anses ha ”huvudansvaret”. Även med beaktande av detta anser vi att det är svårt att formulera en generell regel, utifrån personkategorier, som vid den tidpunkt då en rättelse eventuellt kan behöva göras i ett identitetsindex med någon säkerhet kan peka ut den myndighet som senast har tagit upp biometriska underlag från en viss individ, och som därför skulle kunna ha bäst förutsättningar att rätta en sådan uppgift. En ansvarsfördelning som utgår från en sådan princip förutsätter också att den myndighet som pekas ut har tillgång till en korrekt ansiktsbild eller biometriska uppgifter; för det fall biometriska underlag behöver tas upp för att en rättelse ska kunna ske anser vi att det bör kunna göras av vem som av Polismyndigheten, Migrationsverket eller Skatteverket, i syfte att främja en snabb rättelse. Det är enligt vår mening inte heller osannolikt att den registrerade i praktiken kommer att vända sig med en begäran om att rätta en ansiktsbild eller biometrisk uppgift till den myndighet som han eller hon senast hade kontakt med i ett visst ärende som innebar att uppgifter registrerades eller uppdaterades i ett identitetsindex. En viss naturlig fördelning i ansvaret kan därför antas ske. Det finns naturligtvis inte heller hinder mot att en myndighet i ett enskilt fall, inom ramen för sin serviceskyldighet enligt förvaltningslagen, hänvisar den registrerade till någon av de två andra myndigheterna om man bedömer att en rättelse kan göras snabbare på det sättet.

Vid en sammantagen bedömning av det ovan anförda anser vi att det är mest ändamålsenligt att en ansiktsbild och biometriska upp-

gifter kan rättas eller raderas av Polismyndigheten, Migrationsverket och Skatteverket.

14.4.3 Kontroller när en uppgift behöver rättas eller raderas

Vid en rättelse av en felaktig uppgift måste myndigheten naturligtvis förvissa sig om att rätt individ lokaliseras i ett identitetsindex. Det kan i sig vara en förutsättning för att det i ett enskilt fall överhuvudtaget ska gå att bedöma om en viss uppgift är objektivt felaktig. Kontrollen bör på samma sätt som vi anfört i avsnitt 14.3.7 i första hand göras med biometriska uppgifter. En felaktig uppgift som beror på ett förbiseende eller tekniskt fel kan emellertid också upptäckas utan samband med ett visst ärende där den enskilde är närvarande och har lämnat biometriska underlag. Det kan också vara så att en biometrisk verifiering inte är möjlig i ett visst fall, eftersom det är just dessa uppgifter som är felaktiga. I sådana fall bör en verifiering dock kunna ske på annat sätt, genom en jämförelse med andra uppgifter. Om en felaktighet upptäcks av den myndighet som, enligt våra överväganden i avsnitt 14.4.2, också kan rätta eller radera den felaktiga uppgiften, bör några problem med att verifiera identiteten inte uppstå; det är då, genom att felaktigheten i sig har upptäckts, utrett vilken individ som den felaktiga uppgiften är kopplad till. En särskild verifiering av identiteten kan då tyckas onödig. En rättelse förutsätter emellertid ett den felaktiga uppgiften kan ersättas med en korrekt uppgift. Utifrån vad vi anfört i avsnitt 14.4.1 bör en alfanumerisk uppgift rättas med de uppgifter om individen som finns i folkbokföringsverksamheten eller den centrala utlänningsdatabasen. Det innebär att någon ytterligare kontroll inte är nödvändig i dessa fall. Om det däremot är fråga om att rätta en felaktig ansiktsbild eller biometriska uppgifter kan korrekta sådana uppgifter behöva tas fram genom den enskildes medverkan. I det skedet måste identiteten på den person som lämnar underlagen verifieras. I annat fall finns det risk att felaktigheten rättas med hjälp av underlag som tillhör en annan person. Så får naturligtvis inte ske. Hur verifieringen bör göras beror alltså på omständigheterna i det enskilda fallet och ankommer på den myndighet som rättar uppgiften att bedöma. Huruvida rätt individ har lokaliserats i ett index ankommer också på den myndigheten att ta ställning till.

Om det inte går att verifiera identiteten i ett visst enskilt fall kan detta, som vi ser det, medföra två olika konsekvenser. Om rätt individ inte kan lokaliseras i ett index går det inte heller att konstatera att en viss uppgift är att betrakta som objektivt felaktigt, eftersom det inte går att säkerställa vilka de verkliga förhållanden som uppgiften ska jämföras med utgörs av. I denna situation bör ingen åtgärd vidtas. Om en ansiktsbild eller biometrisk uppgift behöver rättas kan en misslyckad koppling till rätt individ leda till att en objektivt felaktig uppgift inte kan rättas, då det inte går att säkerställa att det finns korrekta uppgifter att rätta felaktigheten med. I detta fall anser vi att en felaktig ansiktsbild eller biometrisk uppgift i stället bör raderas (se avsnitt 14.4.1).

14.4.4 Underrättelseskyldighet avseende felaktiga uppgifter

Vår bedömning

Myndigheter bör inte vara skyldiga att underrätta Polismyndigheten, Migrationsverket eller Skatteverket om det kan antas att en uppgift i ett identitetsindex är felaktig.

Den faktiska möjligheten att rätta en felaktig uppgift som har registrerats i ett identitetsindex är avhängig av att berörd myndighet – Polismyndigheten, Migrationsverket eller Skatteverket – görs uppmärksam på felaktigheten. Myndigheten kan själv upptäcka felaktigheten, exempelvis i samband med att en uppgift uppdateras, men det kan också röra sig om att den registrerade begär att uppgiften ska rättas och därför vänder sig till någon av nämnda myndigheter. En felaktighet kan också uppmärksammas av någon annan myndighet än den som har att rätta en viss uppgift. Frågan är om det bör finnas en skyldighet för andra myndigheter att underrätta Polismyndigheten, Migrationsverket eller Skatteverket om det kan antas att en uppgift i ett identitetsindex är felaktig.

Vi kan konstatera att även utan en särskild underrättelseskyldighet har myndigheter en allmän skyldighet att samverka och bistå varandra. Detta kommer till uttryck i 8 § första stycket förvaltningslagen, där det anges att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter. I för-

arbetena till bestämmelsen framhölls att syftet med bestämmelsen är att samverkan mellan myndigheter ska leda till att förvaltningen generellt ska bli så enhetlig och effektiv som möjligt.[11] Skyldigheten att samverka med andra myndigheter i 8 § förvaltningslagen gäller inte bara vid ärendehandläggning utan även vid annan förvaltningsverksamhet, det vill säga sådan verksamhet som utgör förvaltningsmyndighetens eller domstolens faktiska handlande. Detta kan enligt vår bedömning omfatta verifiering av identitet mot ett identitetsindex. Det bör dock framhållas att samverkansskyldigheten enligt förvaltningslagen inte innebär någon sådan uppgiftsskyldighet som enligt 10 kap. 28 § offentlighets- och sekretesslagen (2009:400) bryter sekretessen mellan myndigheter.[12] Det är därför inte säkert att exempelvis Försäkringskassan – med stöd av 8 § förvaltningslagen – kan informera Skatteverket om att en viss namnuppgift i ett identitetsindex kan antas vara felaktig, utan hänsyn måste tas till eventuell sekretess som gäller för en sådan uppgift. Detta talar för en särskild underrättelseskyldighet, i likhet med vad som gäller i förhållande till oriktiga uppgifter i folkbokföringsverksamheten enligt 32 c § folkbokföringslagen.

Underrättelseskyldigheten i sistnämnda bestämmelse motiveras av att uppgifterna i folkbokföringen inte bara är en förutsättning för Skatteverkets fastställande av skatter utan även för att andra samhällsfunktioner ska ha ett korrekt underlag för beslut och åtgärder. Uppgifter i folkbokföringen kan ligga till grund för bland annat ersättningar och bidrag men även samhällsplanering och forskning. Konsekvenserna av att uppgifterna inte speglar verkliga förhållanden kan vara flera. Exempelvis kan befolkningsstatistiken för vissa geografiska områden bli missvisande och beskattning riskerar att ske på felaktiga grunder. Folkbokföringsuppgifter kan beskrivas som systemöverskridande uppgifter som är centrala i många ersättningssystem för att bedöma rätten till och storleken på ersättningen. Uppgifterna registerförs hos en myndighet, Skatteverket, och används sedan av flera myndigheter. Fel i sådana uppgifter kan leda till felaktiga utbetalningar i flera system.[13]

[11] *En modern och rättssäker förvaltning – ny förvaltningslag*, prop. 2016/17:180, s. 70 ff.
[12] Prop. 2016/17:180, s. 292.
[13] *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, prop. 2020/21:160, s. 23 och *Samlade åtgärder för korrekta utbetalningar från välfärdssystemen*, SOU 2019:59, s. 64 och 76 f.

Även om ett identitetsindex enligt vår bedömning skulle kunna få en central funktion i fråga om verifiering av identitet skulle det inte ha samma funktion som en central källa för information om identiteter som folkbokföringsverksamheten. En felaktighet i ett index kan endast leda till att det inte går att verifiera identitet vid ett visst givet tillfälle, men medför inte några sådana konsekvenser i fråga om exempelvis felaktiga utbetalningar av ekonomiska förmåner som en felaktig uppgift i folkbokföringen kan innebära. Konsekvensen av att en felaktig uppgift behandlas i ett identitetsindex drabbar alltså den enskilde i första hand, inte samhället. Uppgifterna hämtas inte heller in av andra aktörer och används i deras verksamhet på det sätt som sker avseende folkbokföringen, genom Navet och SPAR. Dessa omständigheter talar enligt vår bedömning tydligt mot ett behov av en särskild underrättelseskyldighet.

Sättet på vilket en felaktighet kan uppstå talar som vi ser det också i viss mån mot ett behov av en särskild underrättelseskyldighet. Olika uppgifter i ett index kan nämligen i första hand antas vara felaktiga som en följd av ett tekniskt fel eller ett misstag eller förbiseende av Polismyndigheten, Migrationsverket eller Skatteverket, inte som resultat av ett medvetet agerande av den enskilde. Vi kan vidare konstatera att en uppgift om identitet, identitetsbeteckning eller Migrationsverkets individnummer, enligt våra bedömningar, inte kan anses vara felaktiga på samma sätt som i folkbokföringsverksamheten. Detta med hänsyn till att bedömningen av när en uppgift i respektive system inte stämmer med verkliga förhållanden, och därmed är felaktig i dataskyddsförordningens mening, skiljer sig åt. När det gäller uppgifter i folkbokföringsverksamheten kan dessa vara felaktiga redan när de inte stämmer med faktiska förhållanden som rör den enskilde, exempelvis om han eller hon har flyttat utan att anmäla det till Skatteverket. Alfanumeriska uppgifter i ett identitetsindex är – enligt våra överväganden i avsnitt 14.4.1 – däremot felaktiga först vid den tidpunkt då de inte överensstämmer med motsvarande uppgift i folkbokföringen. För personer som saknar en identitetsbeteckning gäller motsvarande i fråga om alfanumeriska uppgifter i den centrala utlänningsdatabasen respektive ett index. Till detta kommer att en uppdatering av en alfanumerisk uppgift i ett index för personer med en identitetsbeteckning bör göras när en ändring görs i folkbokföringsverksamheten. Den underrättelseskyldighet för myndigheter som följer av 32 c § folkbokföringslagen kommer

därför indirekt att få genomslag även för sådana uppgifter som behandlas i ett identitetsindex. Detta talar enligt vår mening ytterligare mot ett behov av en särskild underrättelseskyldighet.

När det gäller ansiktsbild och biometriska uppgifter bör det för sådana uppgifter – som vi anfört i avsnitt 14.4.1 – endast i undantagsfall alls kunna uppstå felaktigheter, annat än som resultat av ett tekniskt fel. Felaktigheter som beror på tekniska fel kan enligt vår bedömning antas uppmärksammas i första hand av de myndigheter som bör få registrera sådana uppgifter i ett identitetsindex, som då kan vidta åtgärder för att rätta eller radera uppgiften. En skyldighet att underrätta Polismyndigheten, Migrationsverket eller Skatteverket när det kan antas att en ansiktsbild eller biometrisk uppgift är felaktig skulle också kunna leda till att underrättelser sker i onödan, exempelvis för att en biometrisk verifiering inte lyckas vid ett visst tillfälle och myndigheten därför – felaktigt – bedömer att det beror på att det biometriska jämförelsematerialet innehåller fel; det kan för biometriska uppgifter vara betydligt svårare att konstatera att det finns en objektiv felaktighet än vad som är fallet för alfanumeriska uppgifter. Det kan också röra sig om att en handläggare vid en okulär jämförelse mellan ansiktsbilden och den enskilde bedömer att ansiktsbilden inte är välliknande, och därmed felaktig. En underrättelseskyldighet som kan omfatta ett stort antal myndigheter bör som vi ser det inte innefatta sådana bedömningar utan det bör vara förhållandevis enkelt att konstatera att det kan antas finnas en felaktighet. Sammantaget skulle en underrättelseskyldighet – i vart fall om den omfattar ansiktsbild och biometriska uppgifter – riskera att leda till en ökad arbetsbörda, i många fall i onödan.

Den enskilde kan enligt vår bedömning också antas komma att ha ett incitament att på eget initiativ begära rättelse av felaktiga uppgifter i ett identitetsindex med hänsyn till dess ändamål och syfte, nämligen att användas för att biometriskt verifiera identitet i många olika sammanhang; om uppgifterna är felaktiga riskerar en verifiering att misslyckas, på samma sätt som om uppgifter på en fysisk identitetshandling skulle vara felaktiga. Vi bedömer vidare att det saknas incitament för den enskilde att medvetet låta felaktiga uppgifter behandlas i ett index, på det sätt som kan finnas i fråga om uppgifter i andra register och som kan medföra att den enskilde exempelvis får förmåner utbetalade utan att ha rätt till det. Även

dessa omständigheter talar mot ett behov av en särskild underrättelseskyldighet.

Vid en sammantagen bedömning av det ovan anförda anser vi att det saknas ett behov som motiverar att en särskild underrättelseskyldighet införs för myndigheter.

15 Radering av en individ i ett identitetsindex

15.1 Inledning

I kapitel 12 har vi bedömt att ett identitetsindex bör kunna omfatta personer som har en anknytning till Sverige, exempelvis genom bosättning eller hemvist. Motsatsvis skulle en utgångspunkt för överväganden om när en individ bör raderas ur ett identitetsindex därför kunna vara att det ska ske vid en tidpunkt då anknytningen till landet upphör av någon anledning. Behovet av att en individ fortfarande är registrerad i ett identitetsindex skulle då kunna anses ha minskat, eller upphört. Personuppgifter får inte förvaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det följer av principen om lagringsminimering i artikel 5.1 e i dataskyddsförordningen[1]. I detta kapitel utvärderar vi under vilka förutsättningar en individ bör raderas, vilket i praktiken innebär att en identitetsnyckel och samtliga personuppgifter som kan vara kopplade till den i ett visst fall raderas. Radering av enskilda uppgifter som är knutna till en identitetsnyckel behandlas i avsnitt 14.4. I avsnitt 15.2 redogör vi för situationer då en radering kan tänkas aktualiseras på grund av att de yttre förhållandena för en viss individ har förändrats. Den enskilde kan också begära att bli bortglömd, i enlighet med artikel 17 i dataskyddsförordningen. Detta behandlar vi i avsnitt 15.3. I avsnitt 15.4 belyses möjligheten för en tillsynsmyndighet att förelägga om radering av personuppgifter. Ett eventuellt behov av att kunna radera en individ i andra situationer, om det finns särskilda skäl, behandlar vi i avsnitt 15.5.

Att radera en individ ur ett index medför att dennes identitet inte längre kan verifieras mot ett sådant system. Möjligheten att följa en

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

viss individ upphör dessutom och det skydd som en registrering i ett identitetsindex kan ge, genom att utnyttjande av identiteten motverkas, går också förlorat. Utgångspunkten måste därför, som vi ser det, vara att det ska vara tydligt angivet under vilka förutsättningar som en individ bör kunna raderas.

15.2 Radering på grund av ändrade förhållanden

I kapitel 13 har vi bedömt i vilka typer av ärenden en identitetsnyckel bör kunna skapas, utifrån de överväganden vi redogjort för i kapitel 12 avseende behov av att inkludera olika personkategorier i ett index. Det är som vi ser det därför naturligt att i det nu aktuella sammanhanget utgå från ändrade förhållanden som är hänförliga till dessa ärenden; utifrån att en identitetsnyckel exempelvis skapas när någon beviljas ett uppehållstillståndskort som gäller i mer än ett år kan det övervägas att radera en nyckel om uppehållstillståndet upphör att gälla. En radering skulle också kunna föranledas av yttre händelser som inte har någon direkt koppling till det ärendeslag i vilket en identitetsnyckel har skapats.

15.2.1 När den registrerade avlider

Vår bedömning

En individ bör inte raderas ur ett identitetsindex när han eller hon avlider.

Vi kan konstatera att när en person avlider raderas han eller hon inte ur folkbokföringen. Det är viktigt att information om personen finns kvar, exempelvis för att i ett senare skede kunna utreda arvskifte. Syftet med att en person är registrerad i ett identitetsindex är däremot att kunna verifiera hans eller hennes identitet i olika situationer. Den avlidne kan givetvis inte själv uppträda i situationer som innebär att hans eller hennes identitet behöver verifieras. Även avlidna personers identitet kan emellertid riskera att utnyttjas. I förarbetena till bestämmelsen om olovlig identitetsanvändning i 4 kap. 6 b § brottsbalken lyftes fram att det finns risk för att nyligen avlidnas identitetsuppgifter utnyttjas under tiden från dödsfallet till dess att detta har

registrerats i folkbokföringen. Regeringen ansåg däremot att det inte hade framkommit tillräckliga skäl för att utsträcka det straffrättsliga skyddet till att gälla även avlidna personer.[2] En verifiering, särskilt med biometriska uppgifter, mot ett identitetsindex kan som vi ser det emellertid motverka att någon försöker uppträda i den avlidnes identitet; det är inte säkert att den aktör som möter individen i alla situationer kontrollerar mot Navet eller SPAR om personen är avliden och en sådan registrering sker också – som noterades i nyss nämnda förarbeten – med viss fördröjning. Alla personer som enligt våra bedömningar bör kunna registreras i ett identitetsindex kommer inte heller att vara folkbokförda. I förarbetena till lagen (2022:1697) om samordningsnummer noterades att många personer som tilldelats samordningsnummer dessutom kan antas ha avlidit utan att information om detta har kommit Skatteverket tillhanda.[3] Det kan vidare tänkas att en individ som är registrerad i ett index faktiskt inte är avliden, utan att denna omständighet baseras på felaktiga uppgifter eller ett falskt dödsfallsintyg.[4] Det är enligt vår bedömning viktigt att personen då inte kan återkomma och bli registrerad i en annan identitet och på så sätt bryta den möjlighet att följa honom eller henne över tid som ett index syftar till att främja.

Ovanstående talar enligt vår mening starkt mot att en individ bör raderas när han eller hon avlider. Avlidna undantas vidare från dataskyddsförordningens tillämpningsområde, enligt beaktandeskäl 27. Dataskyddsförordningens bestämmelser om skydd för behandling av personuppgifter utgör därför inte hinder mot att *inte* radera en individ som är avliden. Integritetshänsyn skulle dock oavsett kunna tala för att personuppgifter för den som är avliden bör raderas. Det är emellertid fråga om få uppgifter, vilka inte säger något direkt om personen, till skillnad från exempelvis information om civilstånd eller politisk övertygelse. Vi anser därför att uppgifternas karaktär inte i sig kräver att de raderas när någon avlider. Detta särskilt sett i ljuset av det skydd mot identitetsmissbruk, i form av att den avlidnes identitet utnyttjas, som en registrering i ett index kan främja.

Att lagra information i ett index även för avlidna personer kan över tid innebära ökade krav på lagring och teknisk kapacitet. Vi anser dock att behov av lagringsutrymme inte utgör ett tungt väg-

[2] *Straffrättsligt skydd mot olovlig identitetsanvändning*, prop. 2015/16:150, s. 20 f.
[3] *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 93.
[4] Rapport från Brå, *Intyget som dörröppnare till välfärdssystemet*, 2015:8, s. 50 och 61 f.

ande skäl för att radera en individ när han eller hon avlider. Några andra omständigheter som talar mot att fortsatt lagra information om avlidna personer har vi inte funnit. Det bör dock på något sätt markeras i systemet att en viss person är avliden.

15.2.2 När omständigheterna som föranledde registreringen ändras

Vår bedömning

En individ bör inte – förutom vad gäller en kvalificerad skyddsidentitet – raderas ur ett identitetsindex när de omständigheter som föranledde att en identitetsnyckel skapades ändras.

En identitetsnyckel bör enligt våra överväganden i avsnitt 13.3 kunna skapas i vissa ärendeslag, för personer som av olika anledningar kan anses ha en sådan anknytning till Sverige som innebär att deras identitet därför kan behöva verifieras i olika sammanhang. Frågan är om individen bör raderas när de förhållanden som låg till grund för att en identitetsnyckel skapades har upphört eller förändrats av någon anledning. I detta avsnitt redogör vi för ett antal tänkbara sådana situationer. Det kan redan här konstateras att som en följd av vår bedömning ovan att en individ inte bör raderas ens när denne avlider, bör ändrade förhållanden i övrigt sällan kunna antas leda till en sådan åtgärd.

För det första bör en identitetsnyckel, enligt våra överväganden i avsnitt 13.3.5, kunna skapas för den som beviljas ett uppehållstillståndskort med en giltighetstid som överstiger ett år. I avsnitt 12.4.3 har vi gjort bedömningen att det saknas behov av att den som vistas olagligen i Sverige omfattas av ett identitetsindex. Den som befinner sig i landet utan uppehållstillstånd och har meddelats ett verkställbart ut- eller avvisningsbeslut vistas här olagligen. Med hänsyn till att utgångspunkten är att den som har ett gällande avlägsnandebeslut, på eget initiativ, ska lämna landet inom en viss tid kan behovet av att personen är fortsatt registrerad i identitetsindexet antas vara begränsat. Som vi konstaterat i avsnitt 12.4.3 kan emellertid även personer som vistas olagligen i Sverige ha rätt till viss sjukvård, skolgång och bistånd, vilket talar för att det finns ett visst behov av att verifiera identitet även

under denna tid. Detta särskilt med hänsyn till att det är fråga om personer som redan kan ha en anknytning till Sverige på ett sätt som medfört att de registrerats i ett identitetsindex.[5] Det förekommer också att den som vistas i Sverige med gällande avlägsnandebeslut beviljas uppehållstillstånd under tiden som beslutet gäller. Det kan till exempel vara fråga om uppehållstillstånd på grund av verkställighetshinder med stöd av 12 kap. 18 § utlänningslagen (2005:716), uppehållstillstånd som beviljas efter ny prövning med stöd av 12 kap. 19 § samma lag, eller att personen har rätt att vistas i Sverige med stöd av en sådan härledd uppehållsrätt som följer av artikel 20 i EUF-fördraget[6] (se bland annat Migrationsöverdomstolens referat MIG 2023:10 och MIG 2025:4). Att kunna verifiera identitet mot ett index kan också främja verkställighetsarbetet.

Mot bakgrund av dessa omständigheter anser vi att det saknas skäl att radera en identitetsnyckel på grund av att den registrerade individiden har meddelats ett verkställbart avlägsnandebeslut. Inte heller den omständigheten att beslutet verkställs eller upphör att gälla – vilket enligt 12 kap. 22 § utlänningslagen sker fem år efter det att utlänningen har lämnat landet i enlighet med beslutet – medför enligt vår bedömning att individen bör raderas. Vid båda dessa tidpunkter är det möjligt för utlänningen att återvända till Sverige, om han eller hon efter utresan beviljas uppehållstillstånd eller visering (se 12 kap. 23 § utlänningslagen). Även om det i sådana fall finns möjligheter för Polismyndigheten och Migrationsverket att verifiera identitet eller identifiera en individ – på det sätt som redogjorts för i kapitel 7 och avsnitt 8.4.1 – anser vi att det finns fördelar med att över tid kunna följa en individ genom att verifiera identiteten även mot ett identitetsindex.

För personer som registrerats i ett identitetsindex i samband med en anmälan om flyttning till landet och som därmed är folkbokförda skulle det kunna övervägas att radera en identitetsnyckel om personen registreras som utvandrad av Skatteverket. En person som är registrerad som utvandrad kan i många fall antas ha en mer begränsad kontakt med svenska myndigheter; av 20 § folkbokföringslagen framgår att som huvudregel ska den som kan antas komma att regelmässigt tillbringa sin dygnsvila utom landet under *minst ett år* avregistreras

[5] Jfr *Inhibition av verkställigheten*, Ds 2024:23, kapitel 4 och *Preskription av avlägsnandebeslut och vissa frågor om återreseförbud*, SOU 2024:10, s. 45 ff.
[6] Fördraget om Europeiska unionens funktionssätt.

från folkbokföringen som utflyttad. Vi har dock i avsnitt 12.3.1 bedömt att det finns ett behov av att även personer som har varit folkbokförda ska kunna omfattas av ett identitetsindex, med hänsyn dels till att personen behåller sitt personnummer även om en avregistrering sker, dels till att det inte är osannolikt att personen återkommer till Sverige eller på annat sätt behåller en anknytning till landet trots avregistreringen, exempelvis genom ett svenskt medborgarskap. Vi anser därför att en individ inte bör raderas endast på grund av att han eller hon har registrerats som utvandrad av Skatteverket.

En identitetsnyckel bör vidare, enligt våra överväganden i avsnitt 13.3.7, kunna skapas för den som tilldelas ett samordningsnummer eller den vars samordningsnummer förnyas. Enligt 3 kap. 2 § lagen om samordningsnummer ska ett sådant nummer förklaras vilande antingen om någon ansökan om förnyelse inte har kommit in vid utgången av det femte kalenderåret efter det år då numret tilldelades eller senast förnyades, eller om det finns andra skäl för det. Att ett samordningsnummer har förklarats vilande skulle kunna tyda på att individen inte längre har någon anknytning till Sverige, vilket i sin tur kan innebära ett minskat behov av att verifiera hans eller hennes identitet mot ett identitetsindex. I förarbetena till bestämmelserna om vilandeförklaring lyftes dock fram bland annat att samordningsnumret, på motsvarande sätt som ett personnummer, är bestående och unikt genom att det är kopplat till en viss person oavsett om personen exempelvis har lämnat landet eller avlidit, att även ett vilandeförklarat nummer är informationsbärande och finns kvar i folkbokföringen, att det står varje aktör fritt att använda numret även om det har förklarats vilande och att det inte påverkar giltigheten av eventuella resehandlingar som utställts i ett nummer. Att ett samordningsnummer förklaras vilande ansågs inte innebära att en individ per automatik bör avregistreras från de register som en myndighet administrerar.[7] Dessa omständigheter leder enligt vår bedömning till slutsatsen att en individ inte bör raderas i ett index av den anledningen att ett samordningsnummer förklaras vilande.

Vi har i avsnitt 13.3.2–13.3.4 bedömt att en identitetsnyckel bör kunna skapas när ett pass, ett statligt identitetskort eller en statlig e-legitimation utfärdas. Att giltighetstiden för en sådan handling löper ut innebär som vi ser det inte i sig att det skulle finnas ett minskat

[7] Prop. 2021/22:276, s. 48 f.

behov av att kunna verifiera identiteten för innehavaren mot ett identitetsindex. Individen bör därmed inte raderas i dessa situationer.

Slutligen bör en identitetsnyckel, enligt vår bedömning i avsnitt 13.3.1, kunna skapas vid en anmälan eller ansökan om svenskt medborgarskap. Det kan därför övervägas att radera en individ som förlorar sitt svenska medborgarskap, oavsett hur det har förvärvats. Den presumtion för att det genom medborgarskapet finns en sådan anknytning till Sverige att personen också bör omfattas av identitetsindexet som vi bedömt föreligger (se avsnitt 12.3.5) kan då tänkas ha upphört. Ett svenskt medborgarskap kan dock, enligt gällande rätt, förloras endast under vissa mycket specifika förhållanden. Enligt 14 § första stycket lagen (2001:82) om svenskt medborgarskap kan medborgarskapet förloras när en person fyller 22 år, om han eller hon är född utomlands, aldrig har haft hemvist i Sverige och inte varit i landet under förhållanden som tyder på samhörighet med landet. En person som är svensk medborgare och som är eller har varit bosatt i Sverige får inte fråntas sitt svenska medborgarskap, enligt 2 kap. 7 § andra stycket regeringsformen. Vi kan därmed konstatera att personer som, i vart fall enligt gällande rätt, eventuellt kan förlora sitt svenska medborgarskap är personer som bedöms sakna någon egentlig anknytning till Sverige. Det kan med hänsyn till detta, och till att vi i avsnitt 13.4.2 har bedömt att en identitetsnyckel inte bör kunna skapas av en utlandsmyndighet när myndigheten utfärdar ett pass eller en identitetshandling, med fog antas att en person som förlorar sitt svenska medborgarskap inte kommer att vara registrerad i ett identitetsindex. Det talar enligt vår mening mot ett behov av att radera en identitetsnyckel för den som förlorar sitt svenska medborgarskap. Om personen däremot är registrerad tyder det i stället på att han eller hon i vart fall vid registreringstidpunkten hade en anknytning till Sverige. Vi kan här notera att förslag har lämnats i betänkandet *Återkallelse av svenskt medborgarskap* om att ett svenskt medborgarskap ska kunna fråntas den med dubbla medborgarskap som har förvärvat medborgarskapet på felaktiga grunder eller som har begått vissa mycket allvarliga brott.[8] En person som fråntas sitt svenska medborgarskap med stöd av de bestämmelser som föreslagits skulle kunna vara registrerad i ett identitetsindex. Sådana personer kan antas ha en anknytning till Sverige, som innebär att hans eller hennes identitet även i fortsättningen kan behöva verifieras mot ett index.

[8] SOU 2026:21, s. 383 ff.

Vid en sammantagen bedömning av dessa omständigheter anser vi att en individ inte bör raderas endast för att han eller hon förlorar sitt svenska medborgarskap.

Vi har i övrigt – förutom i fråga om kvalificerade skyddsidentiteter (se avsnitt 15.2.3) – inte identifierat någon situation som innebär att ändrade förhållanden avseende den registrerade bör leda till att individen raderas ur ett identitetsindex.

15.2.3 När en kvalificerad skyddsidentitet upphör att gälla

Vår bedömning

En kvalificerad skyddsidentitet bör raderas ur ett identitetsindex när en beslutsmyndighet förordnar om detta i enlighet med 4 § lagen (2006:939) om kvalificerade skyddsidentiteter.

Vi har i avsnitt 13.3.8 bedömt att en identitetsnyckel bör skapas för en kvalificerad skyddsidentitet när ett pass eller ett sådant statligt identitetskort som föreslagits i promemorian *Ett statligt identitetskort*[9] utfärdas och en beslutsmyndighet förordnar om det enligt 4 § lagen (2006:939) om kvalificerade skyddsidentiteter. Syftet med en registrering av en skyddsidentitet i ett identitetsindex är primärt att den som har tilldelats skyddsidentiteten ska kunna utföra sitt arbete på ett fullgott sätt. Ett beslut om kvalificerad skyddsidentitet gäller för den tid som anges i beslutet. Giltighetstiden får bestämmas till högst två år men kan förlängas. Detta framgår av 8 §. Oavsett om giltighetstiden förlängs är beslutet alltså tidsbegränsat och kommer vid en viss tidpunkt att upphöra.

När ett beslut om en kvalificerad skyddsidentitet som innehåller ett förordnande enligt 4 § första stycket 1 eller 2 har upphört att gälla, ska körkort, pass eller andra identitetshandlingar som omfattas av förordnandet lämnas in till beslutsmyndigheten. Om skyddsidentiteten är registrerad i folkbokföringen ska den avregistreras av Skatteverket, efter anmälan från beslutsmyndigheten. Om det fortfarande finns en sådan risk som anges i 3 § 2 får beslutsmyndigheten bestämma att avregistreringen ska anstå till dess att risken har upphört (10 § andra stycket). Att beslutet om en kvalificerad skyddsidentitet

[9] Ju2026/01595.

upphör att gälla innebär därmed att identiteten – som inte svarar mot en riktig person – i praktiken också upphör att existera. Som en följd av detta kan det som vi ser det inte längre finnas något behov av att verifiera skyddsidentiteten mot ett identitetsindex. Vi ser inte heller att det skulle finnas någon sådan risk för identitetskapning som kan göra sig gällande för avlidna personer. Att samma ansiktsbild och biometriska uppgifter förekommer för två identiteter i ett identitetsindex talar också starkt för att en kvalificerad skyddsidentitet bör raderas. Det saknas enligt vår bedömning omständigheter som talar i motsatt riktning.

I likhet med vår bedömning i avsnitt 13.3.8 om när en identitetsnyckel bör skapas, anser vi att beslutsmyndigheten enligt lagen om kvalificerade skyddsidentiteter bör kunna förordna om radering. Det bör i ett sådant förordnande anges vilken myndighet som ska radera skyddsidentiteten ur indexet. Om beslutet som upphört att gälla innehåller ett förordnande enligt 4 § 3 om att den kvalificerade skyddsidentiteten ska folkbokföras bör Skatteverket lämpligen vara ansvarig, och i annat fall Polismyndigheten. Det ankommer dock på beslutsmyndigheten att ta ställning till denna fråga utifrån omständigheterna i det enskilda fallet. Radering av en kvalificerad skyddsidentitet under dessa villkor förutsätter en ändring i 4 §.

15.3 Rätten till radering

Vår bedömning

Det följer av undantaget i artikel 17.3 b i dataskyddsförordningen att den registrerade inte har en rätt att få sina personuppgifter raderade i ett identitetsindex. Detta behöver inte tydliggöras i nationell rätt.

Artikel 17 i dataskyddsförordningen ger som utgångspunkt en rätt för den registrerade att bli bortglömd, det vill säga – i den nu aktuella situationen – att alla uppgifter i ett identitetsindex raderas. Rätten gäller om någon av ett antal uppräknade situationer föreligger. Situationer av intresse i förhållande till ett identitetsindex är, som vi ser det, enligt artikel 17.1 dels a) att personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt

behandlats, dels c) att den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre.

Rätten till radering är inte obegränsad. Enligt artikel 17.3 b i dataskyddsförordningen gäller den till exempel inte i den utsträckning som behandlingen av personuppgifter är nödvändig för att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt, eller för att utföra en arbetsuppgift av allmänt intresse eller som är ett led i myndighetsutövning. I avsnitt 16.3 bedömer vi att verksamhet med ett identitetsindex får anses bedrivas av hänsyn till ett allmänt intresse enligt artikel 6.1 i dataskyddsförordningen. Rätten att bli raderad kan därför inte göras gällande, av den som är registrerad i ett identitetsindex, mot behandlingen av hans eller hennes personuppgifter för dessa ändamål. Det följer alltså av undantaget i artikel 17.3 b dataskyddsförordningen att den registrerade inte har en rätt att få sina personuppgifter i ett identitetsindex raderade och det behöver, enligt vår bedömning, inte tydliggöras i nationell rätt.

Vi kan vidare konstatera att vi i avsnitt 13.2.5 bedömt att registrering inte bör kunna bygga på samtycke; om den registrerade skulle kunna göra gällande rätten till radering skulle innehållet i ett identitetsindex i praktiken bygga på de registrerades kontinuerliga, tysta, samtycke.

15.4 Radering på initiativ av tillsynsmyndigheten

Vår bedömning

Att den myndighet som utövar tillsyn över tillämpningen av dataskyddsförordningen vid behandling av personuppgifter i ett identitetsindex har rätt att förelägga om radering av personuppgifter framgår av artikel 58.2 g i förordningen. Detta behöver därför inte regleras i nationell rätt.

I artikel 58.2 g i dataskyddsförordningen anges att tillsynsmyndigheten bland annat får förelägga om radering av personuppgifter enligt artikel 17, det vill säga i syfte att den registrerade ska raderas ur ett visst register (se avsnitt 15.3). Europeiska dataskyddsstyrelsen

(EDPB) har ansett att tillsynsmyndigheten enligt artikel 58.2 g kan förelägga om radering även utan att den registrerade har begärt radering[10], vilket också slagits fast av EU-domstolen i mål C-46/23, *Újpesti Polgármesteri Hivatal* (punkt 42). Domstolen uttalade också att det gäller oberoende av om personuppgifterna har samlats in från den registrerade själv eller härrör från någon annan källa (punkt 53). Dataskyddsförordningen innehåller inte någon möjlighet att göra undantag från tillsynsmyndighetens befogenheter i detta avseende, eller att i nationell rätt inskränka befogenheterna. Eftersom denna möjlighet att efter föreläggande radera den registrerade följer direkt av dataskyddsförordningen behöver det inte regleras att detta får avse även en individ i ett identitetsindex.

15.5 Särskilda skäl för att radera en individ

Vår bedömning

Polismyndigheten, Migrationsverket och Skatteverket bör få radera en identitetsnyckel och samtliga övriga uppgifter om en individ ur ett identitetsindex om det finns särskilda skäl.

Vi har inledningsvis i det här kapitlet gjort bedömningen att det bör vara tydligt reglerat när en individ bör kunna raderas ur ett identitetsindex, med hänsyn till de effekter som en radering kan få. Det kan emellertid övervägas om det finns ett behov av att systemet medger en viss flexibilitet, för att göra det möjligt att radera en individ även i andra situationer än de som redogjorts för i avsnitt 15.2.3 och 15.4.

En tänkbar situation är att en identitetsnyckel i sig kan anses felaktig. Frågan är emellertid vad som avses med detta. En uppgift som är knuten till en identitetsnyckel bör – enligt våra överväganden i avsitt 14.4 – raderas om den är felaktig, det vill säga om den inte stämmer överens med verkliga förhållanden utifrån de ändamål som den behandlas för och det saknas en korrekt uppgift att ersätta den med. Detta följer direkt av principen om riktighet i artikel 5.1 d i dataskyddsförordningen. När det gäller de uppgifter som är kopplade till en identitetsnyckel i ett identitetsindex kan dessa – om de

[10] EDPB:s yttrande, 39/2021.

är felaktiga – potentiellt ersättas med korrekta uppgifter; exempelvis bör ett namn som är felstavat kunna rättas med uppgifter som finns i folkbokföringen eller den centrala utlänningsdatabasen. För en identitetsnyckel saknas däremot enligt vår mening några sådana potentiellt korrekta uppgifter. Detta då en sådan nyckel endast utgör en unik identifieringsmetod i ett identitetsindex, till vilken uppgifter om individen kopplas. Till skillnad från övriga uppgifter som behöver kunna behandlas i ett index saknas det, som vi ser det, några verkliga förhållanden att jämföra med. Som en följd av detta är det också svårt att dra slutsatsen att en identitetsnyckel kan anses vara felaktig i den mening som avses i artikel 5.1 d i dataskyddsförordningen. Individen som sådan kan enligt vår bedömning inte heller anses vara felaktig på ett sätt som innebär att den kan och ska raderas med stöd av sistnämnda bestämmelse i dataskyddsförordningen.

Med detta sagt skulle en individ och dennes identitetsnyckel dock kunna vara registrerade på felaktiga grunder. Det kan exempelvis röra sig om att en identitetsnyckel har skapats av misstag i ett ärende, att en nyckel har skapats i ett ärendeslag som inte omfattas av uppräkningen i avsnitt 13.3, att det redan fanns en nyckel för individen i fråga (dock med undantag för kvalificerade skyddsidentiteter) som upptäcks i efterhand, eller att det på grund av tekniska problem inte kopplats några biometriska uppgifter till en nyckel i samband med skapandet, och att en ny därför behöver skapas. En felaktig nyckel bör i sådana fall kunna raderas, för att systemet inte ska tyngas av felaktig eller onödig information.

Någon uttömmande uppräkning av när en individ kan ha registrerats felaktigt i ett identitetsindex är enligt vår bedömning inte möjlig att lämna, inte minst med hänsyn till att systemet i nuläget inte existerar. En flexibilitet vad gäller att radera en individ måste emellertid ta i beaktande de effekter som en radering medför och behovet av stabilitet i systemet, på samma sätt som gäller för folkbokföringsverksamheten (se HFD 2019 ref. 9). Ett alternativ för att begränsa möjligheten att radera en individ ur ett index i andra situationer än de i avsnitt 15.2.3 och 15.4 kan vara att ange att det får ske endast om det finns *särskilda skäl*. Ett sådant rekvisit används ibland av lagstiftaren för att markera att det finns ett visst bedömningsutrymme, men att tillämpningen av bestämmelsen förutsätter att det kan motiveras utifrån särskilda omständigheter i det enskilda fallet

och att viss restriktivitet är påkallad.[11] Det ska alltså inte vara fråga om en regelmässig tillämpning.

Även om en möjlighet att radera en individ om det finns särskilda skäl öppnar upp för en tillämpning som är mindre förutsebar än vid en uttömmande uppräkning, bedömer vi att risken för att den används på ett godtyckligt sätt är liten. Sådana risker kan enligt vår bedömning eventuellt göra sig gällande i de fall rekvisitet är kopplat direkt till bedömningen i ett visst ärendeslag, exempelvis om rätten till en sökt förmån eller tillämpningen av ett undantag från en materiell huvudregel är avhängig av att det finns särskilda skäl. Den nu aktuella möjligheten att radera en individ – i första hand i syfte att korrigera misstag och andra felaktigheter i ett identitetsindex – är av helt annat slag och är inte kopplad till något ärende. Vi anser vidare att en möjlighet att radera en individ på grund av att det föreligger särskilda skäl endast bör få användas av de myndigheter som enligt våra bedömningar bör kunna skapa en identitetsnyckel, det vill säga Polismyndigheten, Migrationsverket och Skatteverket. Detta begränsar risken för godtycklighet ytterligare.

Mot denna bakgrund anser vi att Polismyndigheten, Migrationsverket och Skatteverket bör kunna radera samtliga personuppgifter om en individ ur ett identitetsindex om det finns särskilda skäl. Raderingen måste inte göras av den myndighet som har skapat den aktuella identitetsnyckeln, utan kan beslutas av alla tre myndigheter.

[11] Se exempelvis *En straffreform*, SOU 2025:66, s. 1485 och *Effektivare verktyg för att bekämpa brott av unga lagöverträdare*, SOU 2024:93, s. 242.

16 Ett identitetsindex förenlighet med dataskydd m.m.

16.1 Inledning

För att ett system med ett identitetsindex ska kunna skapas och användas för verifiering av identitet och identifiering är det nödvändigt att personuppgifter får behandlas i en sådan verksamhet. Införandet och användningen av ett identitetsindex kommer att innebära en utökad användning av ansiktsbilder och de biometriska uppgifter som kan tas fram ur dessa. Behandlingen av sådana biometriska uppgifter innebär särskilda risker för intrång i den personliga integriteten. Som framgår av redovisningen i kapitel 5 följer det av regeringsformen, Europakonventionen[1] och EU:s rättighetsstadga[2] att vissa förutsättningar måste vara uppfyllda för att det integritetsskydd som regleras i dessa regelverk ska få inskränkas och behandling av biometriska uppgifter vara godtagbar. Vidare ställer dataskyddsförordningen[3] upp krav som ska vara uppfyllda vid behandling av personuppgifter, särskilt vid behandling av så kallade känsliga personuppgifter, såsom biometriska uppgifter. I detta kapitel tar vi ställning till om verksamheten med ett identitetsindex uppfyller de grundläggande förutsättningarna enligt dataskyddsförordningen. Vi utvärderar även om sådan verksamhet utgör en begränsning av rättigheterna i regeringsformen, Europakonventionen och EU:s rättighetsstadga, och om det finns förutsättningar för att begränsa dessa rättigheter. I kapitel 17 gör vi nödvändiga proportionalitetsavvägningar.

[1] Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[2] Europeiska unionens stadga om de grundläggande rättigheterna.
[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

16.2 Utgångspunkter

Det finns i dagsläget inget identitetsindex. Av naturliga skäl bedriver därför inga myndigheter någon verksamhet som är hänförlig till indexet, på det sätt som exempelvis Polismyndigheten bedriver passverksamhet när myndigheten handlägger en ansökan om ett pass. För att kunna ta ställning till om ett system med ett identitetsindex är förenligt med dataskyddsförordningen och skyddet för den personliga integriteten förutsätts bland annat att det går att bedöma om behandlingen av personuppgifter är laglig, det vill säga att den vilar på någon av de rättsliga grunder som anges i artikel 6.1 – och i fråga om känsliga personuppgifter på något av undantagen i artikel 9.2 – i dataskyddsförordningen. Personuppgifter får exempelvis behandlas för att utföra en uppgift av allmänt intresse. Eftersom det idag inte bedrivs någon verksamhet med ett identitetsindex har ingen myndighet fått i uppgift att utföra sådan verksamhet. Med hänsyn till detta behöver det, som vi ser det, därför inledningsvis definieras vad som bör anses utgöra verksamhet med ett identitetsindex.

16.2.1 Verksamhet med ett identitetsindex

Vår bedömning

Med *verksamhet med ett identitetsindex* avses primärt identifiering och skapande av en identitetsnyckel samt verifiering av identitet på förfrågan av de aktörer som bör få kontrollera uppgifter mot ett index. Även andra arbetsuppgifter – bland annat uppdatering, rättelse och radering av uppgifter samt förvaltning av systemet – bör omfattas.

Syftet med ett identitetsindex är att olika samhällsaktörer ska kunna använda det för att verifiera identitet på personer som de möter och, eventuellt, identifiera en person vars identitet inte kan klarläggas. Vi redogör i kapitel 18 och 21 närmare för vem som bör kunna göra detta, och på vilket sätt. Med verksamhet med ett identitetsindex ska förstås den verksamhet som är hänförlig till ett sådant systems funktionalitet i sig. Den innefattar, enligt vår bedömning, tre huvudsakliga delar.

För att ett index ska kunna användas behöver det för det första innehålla individer. En individ bör registreras i ett identitetsindex genom att en identitetsnyckel skapas i något av de ärendeslag och på det sätt som vi beskrivit i avsnitt 13.3. En identitetsnyckel bör kunna skapas av Polismyndigheten, Migrationsverket och Skatteverket, beroende på ärendeslag. När detta görs bedriver myndigheterna därför, enligt vår mening, verksamhet med ett identitetsindex. Detta innefattar den identifiering som vi i avsnitt 18.2.1 bedömer att nämnda myndigheter då behöver genomföra, för att avgöra om en identitetsnyckel ska skapas.

För det andra kan, som vi beskrivit i kapitel 14 och 15, de uppgifter som är kopplade till en viss identitetsnyckel behöva uppdateras, rättas och raderas under vissa förutsättningar. En individ bör också i vissa fall kunna raderas ur indexet, genom att en identitetsnyckel och samtliga uppgifter som är kopplade till den raderas. Även dessa uppgifter bör, enligt våra överväganden, utföras av de ovan nämna myndigheterna. Detta utgör enligt vår mening verksamhet med ett identitetsindex. Även arbete som kan behöva utföras för att förvalta ett system med ett identitetsindex, exempelvis underhåll som krävs för att funktionaliteten ska upprätthållas, bör omfattas.

För det tredje behöver ett system med ett identitetsindex tillhandahålla uppgifter om de individer som är registrerade, när en extern aktör vill verifiera identitet, genom att jämföra uppgifter som har tagits fram med de som finns registrerade. Det är visserligen systemet som sådant som då tillhandahåller informationen, och det innefattar alltså inte några konkreta handläggningsåtgärder i det enskilda fallet som utförs av någon myndighet, på det sätt som sker exempelvis vid en anmälan om ändrad folkbokföring. Något beslut fattas inte heller. Tillhandahållandet av information, och den behandling av personuppgifter som behöver utföras i samband med detta, bedömer vi emellertid också utgör verksamhet med ett identitetsindex. Den eller de myndigheter som bör ansvara för denna automatiska behandling av personuppgifter kommer som vi ser det att bedriva verksamhet med ett identitetsindex när sådan behandling utförs.

Med utgångspunkt i det ovan anförda kan vi redan här konstatera att de myndigheter som kan tänkas bedriva verksamhet med ett identitetsindex i första hand är Polismyndigheten, Migrationsverket och Skatteverket, i vart fall i fråga om verksamhet som omfattar de åtgärder vi redogjort för i kapitel 13–15.

16.3 Rättslig grund för att behandla personuppgifter i verksamheten med ett identitetsindex

Frågan är vilken eller vilka av de rättsliga grunder som framgår av artikel 6 i dataskyddsförordningen som behandlingen av personuppgifter – inklusive känsliga sådana i form av biometriska uppgifter som tagits fram ur en ansiktsbild – i verksamhet med ett identitetsindex kan stödja sig på. I avsnitt 5.2.1 har vi gett en översikt av dataskyddsförordningen. I detta avsnitt utvärderar vi de rättsliga grunder som enligt vår bedömning är relevanta, nämligen allmänt intresse och myndighetsutövning. I avsnitt 16.4 tar vi även ställning till de särskilda krav som gäller för behandling av känsliga uppgifter.

16.3.1 Uppgift av allmänt intresse och myndighetsutövning

Vår bedömning

En myndighet kan tillämpa den rättsliga grunden *uppgift av allmänt intresse* i artikel 6.1 e i dataskyddsförordningen när nödvändig behandling av personuppgifter utförs i verksamheten med ett identitetsindex. När sådan behandling utförs i samband med att en identitetsnyckel skapas, eller när uppgifter som är kopplade till den uppdateras, rättas eller raderas kan en myndighet även tillämpa den rättsliga grunden *myndighetsutövning* i artikel 6.1 e.

När det gäller behandling av personuppgifter för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, med stöd av artikel 6.1 e i dataskyddsförordningen, måste det finnas ett annat stöd i rättsordningen än det som ges i dataskyddsförordningen. Enligt artikel 6.3 ska nämligen den grund för behandlingen som avses i artikel 6.1 e fastställas enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Det krävs inte en reglering i unionsrätten eller i nationell rätt av den personuppgiftsbehandling som ska ske med stöd av dessa rättsliga grunder. Det som måste ha stöd i rättsordningen är i stället uppgiften av allmänt intresse eller rätten att utöva myndighet.[4] En rättslig grund är

[4] *Ny dataskyddslag*, prop. 2017/18:105, s. 49.

fastställd i enlighet med svensk rätt om den följer av författning eller beslut som meddelats i enlighet med regeringsformens bestämmelser.[5]

En uppgift av allmänt intresse kan enligt 2 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, och för myndighetsutövning gäller att denna ska ha stöd i lag eller annan författning. Vi bedömer i avsnitt 16.5.3 att bestämmelser om ett identitetsindex behöver regleras i lag. Därigenom skulle en skyldighet för de myndigheter som bör få bedriva verksamhet med ett identitetsindex vara fastställd i författning.

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen, i fråga om behandling enligt artikel 6.1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en viss behandling av personuppgifter ska anses vara nödvändig måste bedömas från fall till fall, utifrån verksamhetens karaktär. Kravet på att ändamålet ska vara nödvändigt för att utföra en uppgift av allmänt intresse syftar till att utgöra en spärr mot helt onödig behandling av personuppgifter eller sådan behandling som utgör ett oproportionerligt intrång i privatlivet som inte kunnat förutses. Vidare ska unionsrätten eller medlemsstaternas nationella rätt uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. I propositionen *Ny dataskyddslag* konstaterades att bestämmelsen motsvarar det krav som Europakonventionen ställer på lagstiftaren i en rättsstat. Utgångspunkten bör därför vara att kravet är uppfyllt i fråga om bland annat de uppgifter av allmänt intresse som fastställs i enlighet med svensk rätt.[6]

Uppgift av allmänt intresse

I propositionen *Ny dataskyddslag* anförde regeringen bland annat att begreppet uppgift av allmänt intresse måste ges en vid betydelse. Som vi har redogjort för i avsnitt 5.2.3 är alla uppgifter som riksdag

[5] Prop. 2017/18:105, s. 52.
[6] A.a., s. 50 f.

och regering gett statliga myndigheter i uppgift att utföra av allmänt intresse i den mening som avses i dataskyddsförordningen. För det fall en myndighet – det vill säga Skatteverket, Migrationsverket och Polismyndigheten – får i uppgift att bedriva verksamhet med ett identitetsindex och i den verksamheten utför nödvändig behandling av personuppgifter kan den rättsliga grunden uppgift av allmänt intresse därför som utgångspunkt tillämpas. Vi anser vidare att verksamhet med ett identitetsindex i sig är en uppgift av allmänt intresse; syftet med ett sådant system och en sådan verksamhet är att motverka identitetsmissbruk och främja en säker verifiering av identitet; EU-domstolen har i mål C-70/18, *Staatssecretaris van Justitie en Veiligheid mot A m.fl.*, bedömt att målet att förebygga och bekämpa identitets- och dokumentbedrägerier utgör tvingade skäl av allmänintresse. Enligt vår mening utgörs det allmänna intresset av att ovan nämnda myndigheter får behandla personuppgifter i verksamheten med ett identitetsindex av att uppgifterna kan ligga till grund för bättre möjligheter framför allt för olika myndigheter att verifiera identitet för en person som man möter i olika sammanhang, så att myndigheten får ett – i fråga om identitet – korrekt underlag för beslut och åtgärder.[7] Behandlingen av personuppgifterna är därför nödvändig av hänsyn till ett allmänt intresse.

Myndighetsutövning

Frågan är om verksamhet med ett identitetsindex kan anses innefatta myndighetsutövning. Som vi noterat i avsnitt 5.2.3 innebär myndighetsutövning en befogenhet att i förhållande till enskilda bestämma om förmån, rättighet, skyldighet, disciplinär bestraffning eller annat jämförbart förhållande. Befogenheten kan grunda sig på ett konkret beslut av regeringen eller riksdagen men torde vanligtvis grundas på bestämmelser i den offentligrättsliga lagstiftningen som ger en myndighet en rätt eller skyldighet att agera på ett visst sätt. Av naturliga skäl är det i första hand statliga och kommunala myndigheter som ägnar sig åt myndighetsutövning, men även juridiska och fysiska personer kan med stöd av lag anförtros förvaltningsuppgifter som innefattar myndighetsutövning (12 kap. 4 § regeringsformen). I propositionen *Bättre möjligheter att samverka vid med-*

[7] Jfr *Om folkbokföring, samordningsnummer och identitetsnummer*, SOU 2021:57, s. 311.

borgarkontor uttalades bland annat att till myndighetsutövning kan hänföras inte bara beslut som innehåller direkta handlingsmönster i förhållande till den enskilde utan även beslut som har indirekta rättsverkningar, till exempel registreringsbeslut. Karakteristiskt för myndighetsutövning är att den enskilde befinner sig i någon form av beroendeförhållande till myndigheten.[8] Handläggning vid Skatteverket och Försäkringskassan som utmynnar i bindande beslut i form av till exempel folkbokföring eller beviljande av en förmån har ansetts utgöra myndighetsutövning.[9]

En identitetsnyckel bör visserligen skapas i samband med handläggningen av ett ärendeslag som har initierats av den enskilde. Det kan därför sägas att den enskilde indirekt kan påverka huruvida han eller hon registreras i ett index, vilket talar mot att skapandet innebär att den myndighet som gör detta också utövar myndighet. Beslutet att skapa en identitetsnyckel när så är möjligt är emellertid ensidigt och den enskilde bör enligt vår bedömning inte ha någon rätt att invända mot det (se avsnitt 17.3.6). Att registreringen innebär att biometriska uppgifter kommer att behandlas i ett centralt register – vilket enskilda kan tänkas invända mot av olika anledningar – visar enligt vår mening också på ett visst mått av tvång eller beroendeförhållande i förhållande till myndigheten. Att vara registrerad i ett identitetsindex ska också kunna motverka att den registrerades identitet utnyttjas. Registreringen kan på det sättet anses medföra en förmån för den enskilde. En tilldelning av en identitetsnyckel kan enligt vår mening också anses ha likheter med tilldelning av ett person- eller samordningsnummer. Vid en sammantagen bedömning av dessa omständigheter anser vi att skapandet av en identitetsnyckel kan anses utgöra myndighetsutövning, när det görs av Polismyndigheten, Migrationsverket eller Skatteverket. Detsamma bör som vi ser det gälla när uppgifter i ett index som är kopplade till en identitetsnyckel uppdateras, rättas eller raderas, eftersom det också är ett ensidigt handlande från myndighetens sida som kan antas i vart fall påverka den enskilde indirekt, på samma sätt som en registrering.

Övriga åtgärder som ska få vidtas inom ramen för verksamhet med ett identitetsindex – i första hand den automatiska behandling som behöver utföras vid en begäran om verifiering av identitet, men även åtgärder av förvaltande karaktär – utgör däremot enligt vår

[8] Prop. 1996/97:90, s. 26.
[9] SOU 2021:57, s. 463.

bedömning inte myndighetsutövning. Att någons identitet inte kan verifieras i ett enskilt fall kan visserligen tänkas medföra konsekvenser inom ramen för det ärende som föranledde ett behov av att verifiera identiteten. Verifieringen i sig som systemet utför innefattar emellertid inte någon bedömning eller annat handlande inom ramen för verksamheten med ett identitetsindex.

16.4 Behandling av känsliga personuppgifter i verksamheten med ett identitetsindex

För behandling av särskilda kategorier av personuppgifter – i svensk rätt så kallade känsliga personuppgifter – finns särskilda bestämmelser i dataskyddsförordningen. Det gäller bland annat behandling av biometriska uppgifter för att entydigt identifiera en fysisk person. Ett identitetsindex behöver som vi ser det kunna innehålla biometriska uppgifter som tagits fram ur en ansiktsbild. I detta avsnitt tar vi ställning till om behandlingen av sådana uppgifter i verksamheten med ett identitetsindex är tillåten. Några andra känsliga personuppgifter i dataskyddsförordningens mening bör inte få behandlas. Som vi återkommer till i avsnitt 18.5 kommer någon behandling av känsliga personuppgifter inte heller att utföras i verksamheten hos den aktör som vill verifiera identitet mot ett index med hjälp av biometriska uppgifter.

16.4.1 Behandling av biometriska uppgifter

Vår bedömning

Verifiering av identitet med biometriska uppgifter eller identifiering av en person mot ett identitetsindex utgör behandling av känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen.

Behandling av biometriska uppgifter utgör inte alltid behandling av känsliga personuppgifter. Det är när de biometriska uppgifterna behandlas för att entydigt identifiera en fysisk person som det är fråga om behandling av känsliga personuppgifter (artikel 9.1 i dataskydds-

förordningen). Det är alltså av betydelse för vilket ändamål personuppgifterna behandlas.

Vad som avses med behandling för att entydigt identifiera en fysisk person kan diskuteras. Man kan argumentera för att det endast omfattar just *identifiering* av en person, alltså en sökning utifrån biometriska uppgifter för att ta reda på vem personen är, så kallad en-till-många-jämförelse (se avsnitt 7.3.1). Ordalydelsen, *entydigt identifiera*, kan anses tala för denna tolkning.[10] Det går emellertid enligt vår bedömning att argumentera för att artikel 9.1 i dataskyddsförordningen omfattar även v*erifiering* av identitet, det vill säga att biometriska uppgifter jämförs med tidigare lagrade biometriska uppgifter för att kontrollera om en påstådd identitet är riktig, så kallad en-till-en-jämförelse (se avsnitt 7.2.1). En sådan tolkning har som vi ser det stöd i definitionen av biometriska uppgifter, nämligen uppgifter som möjliggör eller *bekräftar* identifieringen av en fysisk person. Vidare har EU-domstolen i mål C-184/20, *OT*, uttalat att en vid tolkning av begreppen *särskilda kategorier av personuppgifter* och *känsliga uppgifter* stöds av syftet med dataskyddsförordningen, vilket är att säkerställa en hög skyddsnivå för fysiska personers grundläggande fri- och rättigheter – särskilt deras rätt till respekt för privatlivet – vid behandling av personuppgifter som rör dem.[11]

Sammantaget bedömer vi att både verifiering av identitet med biometriska uppgifter och identifiering av en person med sådana uppgifter utgör behandling av känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen. Detta inkluderar den identifiering som behöver göras i samband med att en identitetsnyckel skapas (se avsnitt 13.2.1).

16.4.2 Undantag krävs för behandling av biometriska uppgifter

Behandling av känsliga personuppgifter är enligt artikel 9.1 i dataskyddsförordningen som huvudregel förbjuden. I artikel 9.2 finns emellertid en uttömmande uppräkning av undantag, som ska tolkas restriktivt.[12] Med hänsyn till hur undantagen är utformade och vilka situationer de är avsedda att träffa bedömer vi att endast den rättsliga grunden behandling som är nödvändig av hänsyn till ett viktigt

[10] Jfr den engelska versionen; ”for the purpose of uniquely identifying a natural person”.
[11] Se EU-domstolens dom i mål C-184/20, *OT*, punkt 125.
[12] Se till exempel EU-domstolens dom i mål C-252/21, *Meta Platforms Inc*, punkt 76.

allmänt intresse (g) generellt sett kan bli aktuell vid behandling av känsliga personuppgifter i ett system med ett identitetsindex. Vi kommer därför i detta avsnitt endast att ta ställning till om det går att tillämpa detta undantag i dataskyddsförordningen.

16.4.3 Viktigt allmänt intresse

Vår bedömning

Verksamhet med ett identitetsindex kommer att bedrivas av hänsyn till ett viktigt allmänt intresse enligt artikel 9.2 g i dataskyddsförordningen. Den behandling av biometriska uppgifter som är nödvändig för att en myndighet som får i uppdrag att bedriva sådan verksamhet ska kunna utföra den på ett korrekt och effektivt sätt kan därför utföras med stöd av detta undantag i förordningen.

Enligt artikel 9.2 g i dataskyddsförordningen gäller undantag från förbudet i artikel 9.1 om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Närmare om förutsättningarna för att tillämpa undantaget

Undantaget i artikel 9.2 g i dataskyddsförordningen förutsätter att behandlingen av personuppgifter som är nödvändig av hänsyn till ett viktigt allmänt intresse sker på grundval av EU-rätten eller tillämplig nationell rätt, det vill säga att den har ett rättsligt stöd. Detta innebär att den rättsliga grunden för behandlingen ska vara någon av de som avses i artikel 6.1 c eller e, det vill säga bland annat uppgift av allmänt intresse eller myndighetsutövning som har stöd i rättsordningen. Som vi har redogjort för i avsnitt 16.3 krävs det inte en reglering av den personuppgiftsbehandling som ska ske med stöd av dessa rättsliga grunder. Det som måste ha stöd i rättsordningen är i stället den rättsliga förpliktelsen respektive uppgiften av allmänt

intresse eller rätten att utöva myndighet. En rättslig grund är fastställd i enlighet med svensk rätt om den följer av författning eller beslut som meddelats i enlighet med regeringsformens bestämmelser.

Vad som avses med *det väsentliga innehållet i rätten till dataskydd* i artikel 9.2 g definieras inte i dataskyddsförordningen. Regeringen hade svårt att föreställa sig en rättslig grund för behandlingen av personuppgifter som uppfyller kraven i artikel 6, men som ändå inte är förenlig med det väsentliga innehållet i rätten till dataskydd. Om grunden för behandlingen inte är förenlig med det väsentliga innehållet i rätten till dataskydd torde den inte utgöra en godtagbar rättslig grund för behandlingen av personuppgifter överhuvudtaget. Det kunde enligt regeringen därför ifrågasättas om tillägget i artikel 9.2 g utgör ett krav som går utöver de krav som gäller enligt artikel 6 och som måste vara uppfyllda vid all behandling av personuppgifter i allmänt intresse.[13]

Kravet på att det rättsliga stödet ska innehålla bestämmelser om *lämpliga och särskilda skyddsåtgärder* medför att det ofta behövs stöd för själva behandlingen i nationella bestämmelser om personuppgiftsbehandling. I sådana nationella regelverk kan det nämligen finnas bestämmelser om skyddsåtgärder, exempelvis sökbegränsningar och restriktioner för elektronisk åtkomst. Sekretess för de känsliga personuppgifterna kan också vara en skyddsåtgärd. För att undantaget i artikel 9.2 g ska vara tillämpligt ska det rättsliga stödet vidare stå i proportion till det eftersträvade syftet. Vi återkommer i kapitel 17 till proportionalitetsbedömningen.

Verksamhet med ett identitetsindex

Undantaget i artikel 9.2 g i dataskyddsförordningen tillämpas huvudsakligen inom myndigheters verksamhet. Det är svårt att på ett generellt plan definiera vad som skiljer ett allmänt intresse enligt artikel 6.1 e från ett viktigt allmänt intresse enligt artikel 9.2 g. Sådan verksamhet som innefattar myndighetsutövning anses dock vara ett viktigt allmänt intresse. För myndigheters del innefattar detta bland annat den behandling av känsliga personuppgifter som är nödvändig för att de ska kunna utföra sina uppdrag enligt materiell verksamhetslagstiftning och respektive myndighetsinstruktion. När det gäller

[13] Prop. 2017/18:105, s. 84.

myndigheters behandling anses det också utgöra ett viktigt allmänt intresse att svenska myndigheter, även utanför området för myndighetsutövning, kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt.[14]

Ett system med ett identitetsindex syftar till att främja möjligheten att i olika sammanhang säkerställa vem den som en myndighet möter är. En tillförlitlig och solid identitetsförvaltning är av vikt för att motverka och förebygga brott som bygger på att felaktiga identitetsuppgifter och falska identiteter används samt att identiteter kapas eller utnyttjas på annat sätt. Polismyndigheten, Migrationsverket och Skatteverket har en central roll i identitetsförvaltningen, vilket är en anledning till att dessa myndigheter också bör ha en central roll i verksamheten med ett identitetsindex. Vi kan konstatera att dessa myndigheter bedriver verksamheter som motiveras av ett viktigt allmänt intresse.

När det gäller Polismyndighetens möjlighet att verifiera identitet och att identifiera personer vid gränskontroll och inre utlänningskontroll är detta av central betydelse för att principen om en reglerad invandring ska kunna upprätthållas och för att kontrollera att personer som vistas och påträffas i Sverige har rätt att vistas här. För att upprätthålla principen om en reglerad invandring är det också grundläggande att Migrationsverket kan kontrollera enskildas identitet, i första hand i ärenden om uppehållstillstånd; när en person beviljas uppehållstillstånd ligger Migrationsverkets utredning av identiteten också vanligen till grund för registrering av identitetsuppgifter i folkbokföringen. Vidare innefattar Skatteverkets folkbokföringsverksamhet myndighetsutövning. Det utgör även ett viktigt allmänt intresse att folkbokföringen innehåller korrekta uppgifter.[15] Ett identitetsindex ger som vi ser det dessa myndigheter bättre möjligheter att i sina verksamheter säkerställa att en person registreras under endast en identitet, med korrekta uppgifter. Ett index kommer därmed att bli ett verktyg i dessa myndigheters respektive verksamhet. De bör dessutom – vid införande av ett identitetsindex – kunna få i uppgift att bedriva verksamhet med ett identitetsindex, för att indexet ska kunna användas för att motverka identitetsmissbruk i

[14] Prop. 2017/18:105, s. 83.
[15] Jfr *Stärkt kontroll och kvalitet i folkbokföringen,* prop. 2021/22:217, s. 52 och *Stärkt system för samordningsnummer,* prop. 2021/22:276, s. 71.

ett bredare sammanhang, genom att göra det möjligt för andra aktörer att på ett säkert sätt kontrollera att en person man möter är den han eller hon utger sig för att vara.

Det framstår enligt vår mening som givet att det utgör ett viktigt allmänt intresse att myndigheter – i de fall identiteten är av betydelse – kan verifiera identitet på ett säkert sätt. Det är dock inte bara myndigheter som har ett behov av att kunna säkerställa att den person som man möter är den som han eller hon utger sig för att vara; att exempelvis veta vem kunden är har beskrivits som det centrala i förebyggandet av handelsrelaterade former av identitetsmissbruk, exempelvis vid distansköp, vid utlämnande av en vara vid ett utlämningsställe eller vid leverans till beställarens hem- eller företagsadress. Det är alltid till exempel väsentligt att kunna säkerställa att den person som hämtar ut en vara verkligen är eller representerar den som beställt och ska betala för varan. Att en bedragare vid köp- eller lånetillfället utger sig för att vara någon annan än den hon eller han egentligen är anses utgöra en central del i kreditbedrägerier. I en rapport från Brottsförebyggande rådet lyftes bland annat fram att kreditbedrägerier med identitetsstölder är ett växande problem som drabbar näringslivet mycket hårt, men att utnyttjade identiteter även har stora konsekvenser för enskilda.[16] Som vi nämnt i avsnitt 16.3.1 har EU-domstolen i mål C-70/18, *Staatssecretaris van Justitie en Veiligheid mot A m.fl.*, bedömt att målet att förebygga och bekämpa identitets- och dokumentbedrägerier utgör tvingade skäl av allmänintresse. Det kan få långtgående konsekvenser för den enskilde att få sin identitet utnyttjad, och att motverka detta syftar i förlängningen till att tillförsäkra enskilda ett godtagbart skydd för den personliga integriteten (se avsnitt 16.5.2). Att motverka identitetsmissbruk som möjliggör olika former av kreditbedrägerier eller andra typer av utnyttjande av identitet bör därför också som utgångspunkt utgöra ett viktigt allmänt intresse i den mening som avses i artikel 9.2 g i dataskyddsförordningen.

Ett identitetsindex ska ha ett mycket specifikt och avgränsat ändamål, och bör innehålla endast uppgifter som är nödvändiga för att kunna verifiera identitet. En begäran om att verifiera identitet mot ett index har som vi ser det uteslutande som syfte att ge svar på frågan *Är personen den som han eller hon utger sig för att vara?* Ett

[16] Jfr Brå, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag*, Rapport 2016:9, mars 2016, s. 153, 160 och 168 och *Bedrägerier mot privatpersoner*, Rapport 2023:11, s. 43.

index ska alltså inte kunna användas för andra ändamål. Detta tydliggörs av att biometrisk verifiering inte bör kunna genomföras utan medverkan från den vars identitet ska verifieras; det bör alltså inte vara möjligt för en aktör att begära verifiering mot indexet ensidigt, exempelvis för att systematiskt få tillgång till uppgifter från systemet för att bygga upp ett eget register eller göra sökningar ”i onödan”. Det saknas som vi ser det alltså anledning att begära verifiering av någon annan anledning än att kontrollera identitet, i syfte att kunna motverka sådana typer av identitetsmissbruk som nämnts ovan och för att skydda enskilda från att deras identiteter utnyttjas.

Vi anser mot denna bakgrund att verifiering av identitet mot ett identitetsindex som utgångspunkt alltid får anses ske av hänsyn till ett viktigt allmänt intresse. Tillämpning av undantaget i artikel 9.2 g i dataskyddsförordningen förutsätter dock att den behandling av biometriska uppgifter som utförs står i proportion till det eftersträvade syftet med behandlingen. I kapitel 17 återkommer vi till frågan om en verksamhet med ett identitetsindex kan anses vara proportionerlig. En viktig del vid en sådan proportionalitetsbedömningen är vilka aktörer som bör få verifiera identitet biometriskt mot indexet och under vilka förutsättningar en verifiering då får göras. Det återkommer vi till i kapitel 21.

I de fall en identifiering behövs för att kunna avgöra om en identitetsnyckel behöver skapas får det också anses utgöra ett viktigt allmänt intresse att en sådan identifiering kan genomföras (se avsnitt 18.2.1). Om ett index införs kommer det, enligt vår bedömning, även att kunna främja att myndigheter kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt, också utanför området för myndighetsutövning. Även detta utgör, som framgår av förarbetena till dataskyddslagen, ett viktigt allmänt intresse. Med hänsyn till detta och till vad som anförts ovan anser vi vid en sammantagen bedömning att verksamheten med ett identitetsindex kan bedrivas av hänsyn till ett viktigt allmänt intresse. Den behandling som är nödvändig för att en myndighet som ges i uppgift att bedriva sådan verksamhet ska kunna utföra den på ett korrekt och effektivt sätt har därmed, enligt vår mening, stöd i undantaget i artikel 9.2 g i dataskyddsförordningen.

16.5 Förhållande till grundläggande rättigheter

Det finns alltså som vi ser det rättslig grund enligt dataskyddsförordningen för behandling av personuppgifter i verksamheten med ett identitetsindex och ett tillämpligt undantag för behandling av känsliga personuppgifter, det vill säga biometriska uppgifter. Behandlingen av biometriska uppgifter innebär emellertid ofta särskilda risker för intrång i den personliga integriteten och därmed också i de rättigheter i fråga om skydd för privatlivet som följer av regeringsformen, Europakonventionen och EU:s rättighetsstadga. Behandling som inskränker grundläggande rättigheter kan dock vara tillåten, om den kan motiveras av ett legitimt mål, exempelvis av ett allmänt samhällsintresse. Vi belyser i detta avsnitt dessa frågor.

16.5.1 Behandling av biometriska uppgifter i verksamhet med ett identitetsindex inskränker vissa rättigheter

Vår bedömning

Verksamhet med ett identitetsindex, som innebär att biometriska uppgifter som tagits fram ur ansiktsbilder från ett stort antal personer behandlas, utgör en inskränkning av de rättigheter som följer av regeringsformen, Europakonventionen och EU:s rättighetsstadga.

Vi har i kapitel 11 redogjort för vilka typer av personuppgifter som bör få behandlas i ett system med ett identitetsindex. När det gäller känsliga personuppgifter har vi i avsnitt 11.4.5 bedömt att det visserligen kan finnas fördelar med att ett identitetsindex innehåller biometriska uppgifter som kan tas fram ur såväl fingeravtryck som ur ansiktsbild. Bland annat med hänsyn till de överväganden kring proportionalitet som vi gör i kapitel 17 har vi emellertid bedömt att fingeravtryck och sådana biometriska uppgifter som kan tas fram ur dem *inte* bör kunna behandlas i ett identitetsindex. Några andra känsliga personuppgifter, i den mening som avses i 3 kap. 1 § dataskyddslagen, än sådana biometriska uppgifter som kan tas fram ur en ansiktsbild kommer därmed inte att få behandlas i verksamheten med ett identitetsindex. Det skydd mot påtvingat kroppsligt ingrepp

som framgår av 2 kap. 6 § första stycket regeringsformen kommer därför inte att begränsas genom verksamheten (jfr avsnitt 5.3.1)

Behandlingen av biometriska uppgifter i verksamheten med ett identitetsindex kommer däremot, enligt vår bedömning, att innebära en inskränkning i det skydd för den personliga integriteten samt rätten till respekt för privatlivet som följer av 2 kap. 6 § andra stycket regeringsformen, artikel 8 i Europakonventionen och artikel 7 och 8 i EU:s rättighetsstadga, av följande skäl.

Privatliv är en bred term som inte går att uttömmande definiera. Det omfattar dock både fysisk och personlig integritet. Europadomstolen har i flera fall konstaterat att artikel 8 ålägger medlemsstaterna 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 exempelvis *Airey mot Irland,* nr 6289/73, *X och Y mot Nederländerna*, nr 8978/80 och *Söderman mot Sverige*, nr 5786/08). Att ta någons fingeravtryck utgör ett intrång i privatlivet (se *S. och Marper mot Storbritannien*, nr 30562/04 och 30566/04). Detsamma gäller att ta fotografier av en person utan dennes samtycke (se *von Hannover mot Tyskland*, nr 59320/00). Redan att en myndighet behandlar eller registrerar uppgifter om en persons privatliv, det vill säga personuppgifter, kan i vissa fall utgöra en inskränkning av rätten till skydd för privatlivet (se Europadomstolens avgörande i *Leander mot Sverige*, nr 9248/81). I målet *S. och Marper mot Storbritannien* uttalade Europadomstolens att skyddet av personuppgifter är av grundläggande betydelse för en persons åtnjutande av sin rätt till respekt för privat- och familjeliv och att behovet av lämpliga skyddsåtgärder i nationell rätt är desto större när det gäller skydd av personuppgifter som genomgår automatisk behandling. Av EU-domstolens praxis avseende begränsning av de rättigheter som följer av artikel 7 och 8 framgår sammantaget att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är absolut nödvändigt (se de förenade målen C-203/15 och C-698/15, *Tele2 Sverige AB och Secretary of State for the Home Department mot Post- och telestyrelsen m.fl.* och mål C-140/20, *G.D. mot Commissioner of the Garda Síochána m.fl.*).

Att ta en ansiktsbild av en person utan hans eller hennes samtycke kan alltså i sig anses utgöra ett intrång i privatlivet.[17] Behandlingen

[17] *Biometri i brottsbekämpningen*, prop. 2024/25:37, s. 47.

av biometriska uppgifter som kan tas fram ur bilden får därför också anses kunna utgöra en inskränkning i privatlivet i den mening som avses i artikel 8 i Europakonventionen och artikel 7 och 8 i EU:s rättighetsstadga. Frågan om inskränkningen kan motiveras med hänsyn till ett legitimt mål, och är proportionerlig, återkommer vi till i avsnitt 16.5.2 och kapitel 17.

Behandling av de biometriska uppgifter som kan tas fram ur en ansiktsbild behöver få utföras utan den registrerades samtycke, för att ett system med ett identitetsindex ska vara funktionellt. Det gäller både vid skapandet av en identitetsnyckel och när uppgifter behandlas i verksamheten efter en begäran om att verifiera identitet. Verksamheten med ett identitetsindex kan som vi ser det därför även anses utgöra en inskränkning i det skydd mot intrång i den personliga integriteten som följer av 2 kap. 6 § andra stycket regeringsformen. Enligt bestämmelsen är var och en skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Med begreppet *enskilds personliga förhållanden* avses samma som i tryckfrihetsförordningen och offentlighets- och sekretesslagstiftningen, vilket innebär att till exempel uppgifter om namn och andra identifikationsuppgifter och fotografier omfattas.[18] Exempel på uppgiftssamlingar som innebär en kartläggning är misstanke- och fingeravtrycksregister.

När det gäller skyddet i 2 kap. 6 § andra stycket regeringsformen mot intrång i skyddet för den personliga integriteten kan vi konstatera att det enbart omfattar *betydande* integritetsintrång. Denna begränsning motiveras av att grundlagsskydd är motiverat enbart i fråga om övervakning eller kartläggning som är av särskilt ingripande karaktär och som har viss intensitet eller omfattning.[19] Behandlingen av uppgifter i verksamheten med ett identitetsindex får enligt vår mening anses innebära en kartläggning eftersom ett index, enligt våra bedömningar, behöver innehålla uppgifter om identitet, identitetsbeteckning och ansiktsbilder.[20]

Den avgörande frågan är därmed om det intrång i den personliga integriteten som behandlingen kan innebära är betydande. Vad som är ett betydande intrång i den personliga integriteten får bedömas

[18] A.a., s. 47.
[19] *En reformerad grundlag*, prop. 2009/10:80, s. 182.
[20] Jfr *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning*, Ds 2019:5, s. 89.

utifrån åtgärdens intensitet och omfattning samt uppgifternas integritetskänsliga natur. Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning av den enskildes personliga förhållanden är inte åtgärdens huvudsakliga syfte, utan vilken effekt den har. Vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden är det naturligt att stor vikt läggs vid uppgifternas karaktär. Ju känsligare uppgifterna är, desto mer ingripande måste det allmännas hantering av uppgifterna normalt anses vara. Även hantering av ett fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen är det även naturligt att stor vikt läggs vid ändamålet med behandlingen. Även mängden uppgifter kan vara en betydelsefull faktor i sammanhanget.[21]

I betänkandena *Folkbokföringsverksamhet, biometri och brottsbekämpning* och *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll* bedömdes behandling av ansiktsbilder och fingeravtryck samt biometriska uppgifter som tas fram ur dessa – i samband med en identitetskontroll i folkbokföringsverksamheten och vid en ansökan om uppehållstillstånd – utgöra ett betydande intrång i den personliga integriteten.[22] I sistnämnda betänkande beräknades att antalet fingeravtryck som lagras i Migrationsverkets register skulle komma att kunna öka från cirka 275 000 till cirka tre miljoner. I promemorian *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* samt betänkandena *Ett säkert statligt ID-kort – med e-legitimation* och *En säker och tillgänglig statlig e-legitimation* gjordes motsatt bedömning i fråga om integritetsintrång.[23] I sistnämnda utredningar beaktades bland annat att personuppgifterna skulle behandlas med anledning av handläggningen av ett ärende, att pass- och id-kortsverksamheten inte kan betraktas som särskilt integritetskänslig, att det stora flertalet av uppgifterna inte är av känslig karaktär och att de biometriska uppgifter som tagits fram ur ansiktsbilder endast i begränsad omfattning skulle kunna användas för sökningar.

Vi kan konstatera att den behandling av känsliga personuppgifter som kan behöva utföras i verksamheten med ett identitetsindex inte

[21] Prop. 2009/10:80, s. 180 ff.
[22] Se SOU 2025:75, s. 429 ff. och SOU 2024:80, s. 478.
[23] Se Ds 2019:5, s. 90, SOU 2019:14, s. 223 och SOU 2023:61, s. 123.

har ett direkt samband med eller är nödvändig för handläggningen av ett visst ärende, på samma sätt som vid en ansökan om pass eller identitetskort. Detta får anses vara en väsentlig skillnad. Vidare skulle – med utgångspunkt i våra bedömningar i kapitel 12 och 13 – ett identitetsindex relativt snabbt komma att innehålla biometriska uppgifter om ett mycket stort antal personer, och målsättningen enligt våra direktiv är att så många som möjligt som vistas i Sverige på sikt ska kunna ingå i ett system för stärkt verifiering av identitet. Det kan alltså bli fråga om lagring av biometriska uppgifter för flera miljoner personer, fler än de vars biometriska uppgifter är lagrade i passregistret eller det pass- och identitetskortsregister som har föreslagits.[24] Redan dessa omständigheter talar enligt vår bedömning starkt för att verksamheten med ett identitetsindex utgör ett betydande intrång i den personliga integriteten. När det gäller typer av uppgifter skulle visserligen inga andra känsliga uppgifter än biometriska uppgifter från ansiktsbilder behöva behandlas. Person- och samordningsnummer ska däremot också få behandlas. Även om sådana uppgifter inte är att anse som känsliga uppgifter i dataskyddsförordningen mening har de – som vi redogjort för i avsnitt 5.2.5 – en särställning, och kräver att särskilda avvägningar görs mellan integritetsintrånget och ändamålet med behandlingen. Detta bör enligt vår mening också vägas in.

Vid en sammantagen bedömning – där vi framför allt har beaktat den stora mängd biometriska uppgifter som skulle behöva behandlas – anser vi att verksamheten med ett identitetsindex får anses utgöra ett betydande intrång i den personliga integriteten på det sätt som avses i 2 kap. 6 § andra stycket regeringsformen. Verksamheten utgör, enligt vår bedömning, även en inskränkning i skyddet för privatlivet enligt Europakonventionen och EU:s rättighetsstadga.

[24] *Ett statligt identitetskort*, Ju2026/01595, s. 129.

16.5.3 Inskränkningarna har ett legitimt syfte

Vår bedömning

Verksamheten med ett identitetsindex syftar till och är ägnad att motverka identitetsmissbruk, som är ett mål av allmänt samhällsintresse som erkänns av unionen. Behandling av personuppgifter i en sådan verksamhet skulle utföras för ändamål som är godtagbara i ett demokratiskt samhälle.

Frågan är om det finns legitima skäl som kan motivera de inskränkningar som vi ovan bedömt att verksamhet med ett identitetsindex skulle medföra, dels i skyddet för privatlivet enligt Europakonventionen och EU:s rättighetsstadga, dels i skyddet för den personliga integriteten enligt regeringsformen.

Verksamheten utgör ett allmänt samhällsintresse

Beträffande EU:s rättighetsstadga framgår av artikel 52.1 att begränsningar, med beaktande av proportionalitetsprincipen, får göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter. EU-domstolen har uttalat att en balanserad avvägning ska göras, mellan å ena sidan målet av allmänt samhällsintresse och å andra sidan de berörda rättigheterna, för att säkerställa att de olägenheter som åtgärder medför inte är orimliga i förhållande till de eftersträvade målen. Möjligheten att motivera en inskränkning ska bedömas utifrån allvaret i det ingrepp som den medför, och genom en prövning av om betydelsen av det mål av allmänt intresse som eftersträvas med denna begräsning står i proportion till ingreppets allvar (se EU-domstolens dom i mål C-61/22, *Landeshaupstadt Wiesbaden*, punkt 83). Ett mål av allmänt samhällsintresse kan inte, oavsett hur betydelsefullt det är, i sig ensamt motivera en begränsning av en grundläggande rättighet (se EU-domstolens dom i mål C-293/12, *Digital Rights Ireland Ltd v Ireland*), utan en proportionalitetsavvägning måste alltid göras.

Vi har i kapitel 9 beskrivit olika typer av identitetsmissbruk. Utnyttjade och kapade identiteter är ett allt större problem och bedöms vara mer omfattande än renodlat falska identiteter. Verksamheten

med ett identitetsindex skulle enligt vår mening främja en stärkt koppling mellan en grundidentitet som har etablerats av Polismyndigheten, Migrationsverket eller Skatteverket i olika situationer, och en verifiering av identitet, med grund i biometriska uppgifter. Syftet med en sådan verksamhet är att motverka identitetsmissbruk och ger framför allt myndigheter utökade möjligheter att verifiera identitet för en person som myndigheten möter i olika sammanhang. Kontroll av biometriska uppgifter mot ett identitetsindex kan förhindra dels att en person uppträder under olika identiteter vid kontakt med myndigheter, dels att multipla identiteter registreras för en och samma person, i till exempel folkbokföringsverksamheten. Verksamheten med ett identitetsindex syftar alltså inte bara till att motverka identitetsmissbruk utan är också ägnad att uppnå detta syfte genom de möjligheter till verifiering av identitet som ett identitetsindex skulle ge vid ett införande.

Att motverka identitetsmissbruk och främja en säker verifiering av identitet är enligt vår bedömning viktigt från samhällssynpunkt, exempelvis för att förhindra brott mot välfärdssystemen; hur identitetsmissbruk används för sådana syften har belysts bland annat i betänkandet *Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen*.[25] Detta får även stöd i praxis från EU-domstolen. I mål C-291/12, *Schwarz*, konstaterade domstolen att det utgör ett mål av allmänt samhällsintresse som erkänns av unionen att förbygga att pass förfalskas samt att förhindra att de används i bedrägligt syfte. Detta bekräftades i mål C-61/22, *Landeshaupstadt Wiesbaden*. I domen anförde EU-domstolen bland annat att lagstiftaren inte är skyldig att vänta på att antalet missbruk av identitetshandlingar ska öka till en viss nivå, utan tvärtom har en rätt att förekomma en sådan utveckling, bland annat av riskhanteringsskäl, under förutsättning att de övriga kraven enligt proportionalitetsprincipen är uppfyllda (se punkt 119–122). I mål C-70/18, *Staatssecretaris van Justitie en Veiligheid mot A m.fl.,* bedömde EU-domstolen att målet att förebygga och bekämpa identitets- och dokumentbedrägerier utgör tvingade skäl av allmänintresse. Flera av de lagstiftningsåtgärder på EU-nivå som har genomförts under senare år syftar också uttryckligen till att bland annat främja verifiering av identitet och bekämpa identitets-

[25] SOU 2020:35, s. 146 ff.

bedrägeri och missbruk av resehandlingar, vilket enligt vår mening visar på att det är ett prioriterat och allmänt samhällsintresse.[26]

Vi kan vidare konstatera att det enligt 4 kap. 6 b § brottsbalken är straffbart att olovligen använda en annan persons identitetsuppgifter och utge sig för att vara honom eller henne. I förarbetena till bestämmelsen anfördes att det fanns behov av att kriminalisera detta, med hänsyn till att det kan få långtgående konsekvenser för den enskilde att få sin identitet utnyttjad och till Europakonventionens krav på att tillförsäkra enskilda ett godtagbart skydd för den personliga integriteten.[27] Verksamheten med ett identitetsindex kan, om ett sådant system införs, som vi ser det främja att denna typ av brottslighet motverkas, vilket enligt vår bedömning ytterligare visar på att verksamheten skulle vara viktig ur samhällssynpunkt. Till detta kommer, enligt vår bedömning, att möjligheten att genom ett identitetsindex främja en säker verifiering av identitet bidrar till en ökad trygghet för enskilda genom att deras identitet inte kan utnyttjas av någon annan.

Sammantaget anser vi att verksamheten med ett identitetsindex svarar mot ett sådant mål av allmänt samhällsintresse som erkänns av unionen och som avses i artikel 52.1 i EU:s rättighetsstadga.

Verksamheten tillgodoser ändamål som är godtagbara i ett demokratiskt samhälle

När det gäller Europakonventionen ger artikel 8.2 vissa möjligheter att inskränka skyddet för privat- och familjelivet, om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten eller landets ekonomiska välstånd eller till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter. Enligt 2 kap. 21 § regeringsformen får begränsningar enligt 20 § av grundläggande fri- och rättigheter göras endast för ändamål som är godtagbara i ett demokratiskt samhälle.

Av praxis från Europadomstolen framgår att en nationell författning som innebär en sådan inskränkning måste uppfylla vissa mini-

[26] Se exempelvis artikel 6.1 i in- och utreseförordningen (Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017) och artikel 2.2 b IOF (Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019).
[27] *Straffrättsligt skydd mot olovlig identitetsanvändning*, prop. 2015/16:150, s. 13.

mikrav i fråga om kvalitet och tydlighet. Att ett ingripande ska vara nödvändigt i ett demokratiskt samhälle innebär att det ska finnas ett angeläget samhälleligt behov av åtgärden i fråga. I det ligger bland annat en begränsning som innebär att inskränkningen inte får gå längre än vad som är nödvändigt med beaktande av proportionalitetsprincipen, det vill säga den ska stå i rimlig relation till det intresse som åtgärden är avsedd att tillgodose (se Europadomstolens avgöranden i målen *S. och Marper mot Storbritannien* och *Glukhin mot Ryssland*) (se även kapitel 17 i detta avseende). Regeringen anförde i propositionen *Anpassning av svensk rätt till den reviderade VIS-förordningen* att intresset av att motverka identitetsbedrägerier och att fastställa identiteten på de personer som vistas i Sverige är ändamål som är godtagbara i ett demokratiskt samhälle, med hänsyn till förebyggande av nationell och allmän säkerhet samt förebyggande av oordning.[28] Utifrån vad vi anfört ovan om syftet och målet med verksamheten med ett identitetsindex anser vi att det saknas anledning att ha en annan utgångspunkt i fråga om den verksamheten.

De inskränkningar av rättigheter som verksamheteten med ett identitetsindex medför får, enligt vår bedömning, anses tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, i den mening som avses i bestämmelsen i 2 kap. 21 § regeringsformen och i artikel 8.2 i Europakonventionen.

16.5.4 Verksamheten med ett identitetsindex bör regleras i lag

Vår bedömning

Verksamheten med ett identitetsindex, och användningen av systemet, bör regleras i lag.

Den inskränkning i skyddet för den personliga integriteten – som följer av regeringsformen, Europakonventionen och EU:s rättighetsstadga – som verksamheten med ett identitetsindex innebär, måste regleras på ett tydligt sätt. Behandling av känsliga personuppgifter som är nödvändig av hänsyn till ett viktigt allmänt intresse måste för att vara tillåten ske på grundval av EU-rätten eller tillämplig nationell rätt, det vill säga den måste ha ett rättsligt stöd. Detta inne-

[28] Prop. 2024/25:176, s. 44.

bär dock inte ett att det finns krav på att själva behandlingen av personuppgifter måste regleras. Det är i stället uppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen.[29] Författningsstödet måste vara förutsebart och formulerat så att enskilda kan anpassa sitt beteende efter det. Utrymmet för skönsmässig tillämpning måste vara tillräckligt tydligt avgränsat. Vidare har det i äldre förarbeten om bland annat integritetsskyddet för uppgifter i personregister påpekats att myndighetsregister som innehåller ett stort antal registrerade och har ett särskilt känsligt innehåll bör regleras i lag.[30] Av 2 kap. 20 § regeringsformen framgår uttryckligen att skyddet mot intrång som innebär kartläggning av den enskildes personliga förhållanden endast får begränsas i lag.

För att verksamheten med ett identitetsindex ska kunna vara förenlig med dels grundläggande rättigheter, dels dataskyddsförordningen, behöver det alltså finnas rättsligt stöd i lag för berörda myndigheter att bedriva sådan verksamhet, om ett system med ett identitetsindex skulle införas. Utifrån hur vi har definierat verksamhet med ett identitetsindex i avsnitt 16.2.1 innebär det att det i lag tydligt behöver anges vem som får ta upp ansiktsbilder och behandla de biometriska uppgifter som kan tas fram ur dessa för att exempelvis skapa en identitetsnyckel, och under vilka förutsättningar detta får ske.[31] Även möjligheten för olika aktörer att – på det sätt som vi beskriver i kapitel 18 och 21 – använda ett identitetsindex för att verifiera identitet eller, i vissa fall, identifiera en person behöver enligt vår bedömning regleras i lag.

[29] Prop. 2017/18:105, s. 48.
[30] Regeringens proposition 1990/91:60 om offentlighet, integritet och ADB, s. 58.
[31] Jfr SOU 2024:80, s. 453.

16.6 Sammanfattande slutsatser

Vår bedömning

Förenlighet med dataskyddsförordningen och grundläggande rättigheter förutsätter att verksamheten med ett identitetsindex regleras i lag samt innehåller skyddsåtgärder och utformas på ett sådant sätt att verksamheten inte går utöver vad som är nödvändigt för att uppnå målet att på ett säkert sätt kunna verifiera identitet och identifiera personer.

Vi har ovan bedömt att det finns en rättslig grund enligt dataskyddsförordningen för att behandla personuppgifter i verksamheten med ett identitetsindex. När det gäller biometriska uppgifter anser vi att dessa kan behandlas av hänsyn till ett viktigt allmänt intresse. Det kan därmed vara tillåtet enligt dataskyddsförordningen att behandla biometriska uppgifter inom ramen för verksamheten med ett identitetsindex, om övriga förutsättningar i artikel 9.2 g för sådan behandling är uppfyllda. Vidare har vi bedömt att verksamheten med ett identitetsindex syftar till och är ägnad att motverka identitetsmissbruk, vilket är ett mål av allmänt samhällsintresse som erkänns av unionen. Behandlingen av biometriska uppgifter skulle dessutom utföras för ändamål som får anses godtagbara i ett demokratiskt samhälle. Det innebär att den begränsning av rättigheter som verksamheten medför kan vara förenlig med regeringsformen, Europakonventionen och EU:s rättighetsstadga, om förutsättningarna i övrigt för begränsning är uppfyllda.

Förenlighet med dataskyddsförordningen och sistnämnda rättigheter förutsätter emellertid även att regelverket avseende verksamheten införs i lag. Det kan även behöva finnas särskilda skyddsåtgärder i form av exempelvis sekretessbestämmelser. Det krävs också att regleringen av verksamhet med ett identitetsindex – och användningen av ett sådant system – utformas på ett sätt som inte går utöver vad som är nödvändigt för att uppnå målet med den. Målet av allmänt samhällsintresse som eftersträvas ska stå i proportion till ingreppets allvar. I kapitel 17 redogör vi för hur denna proportionalitetsbedömning ska gå till och vilka omständigheter vi beaktar vid bedömningen.

17 Proportionalitetsbedömning avseende ett identitetsindex

17.1 Inledning

Vi har i kapitel 16 bedömt att verksamheten med ett identitetsindex begränsar vissa rättigheter enligt regeringsformen, Europakonventionen[1] och EU:s rättighetsstadga[2], men att verksamheten syftar till och är ägnad att uppnå mål av allmänt samhällsintresse som erkänns av unionen. Vidare får inskränkningen av rättigheter som behandlingen av personuppgifter i en sådan verksamhet medför, enligt vår bedömning, anses ske för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. I föregående kapitel har vi också bedömt att behandlingen av biometriska uppgifter i verksamheten med ett identitetsindex kan utföras av hänsyn till ett viktigt allmänt intresse enligt artikel 9.2 g i dataskyddsförordningen.

För att kunna ta ställning till om verksamhet med ett identitetsindex är förenlig med grundläggande rättigheter och med dataskyddsförordningen förutsätts emellertid även att en proportionalitetsbedömning görs. Hur denna bedömning ska gå till och vilka omständigheter som ska beaktas i det aktuella sammanhanget redogör vi för i detta kapitel. Utformningen av ett system med ett identitetsindex kräver proportionalitetsavvägningar även när det gäller till exempel under vilka förutsättningar olika aktörer bör få ta upp biometriska underlag för att kunna göra kontroller av biometriska uppgifter mot uppgifter i ett identitetsindex. Vi återkommer till dessa frågor i kapitel 18 och 21.

[1] Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[2] Europeiska unionens stadga om de grundläggande rättigheterna.

17.2 Utgångspunkter för bedömningen

Proportionalitetsprincipen aktualiseras vid en inskränkning av de rättigheter som framgår av regeringsformen, Europakonventionen och EU:s rättighetsstadga. Principen innebär att de åtgärder som vidtas av det allmänna inte får vara mer ingripande än vad som är nödvändigt för att uppnå syftet med åtgärderna, och kommer till uttryck på olika sätt i dessa regelverk, vilket vi redogjort för i avsnitt 5.3 och i kapitel 16. Ett sätt att uttrycka proportionalitetsbedömningen, enligt artikel 8.2 i Europakonventionen, är att det ska finnas ett rimligt förhållande mellan hur stort ingreppet i den enskildes rätt är och hur starkt det behov är som ska tillgodoses genom ingreppet; endast då kan ingreppet anses nödvändigt i ett demokratiskt samhälle.[3]

När det gäller dataskyddsförordningen krävs att behandlingen av känsliga personuppgifter med hänsyn till ett viktigt allmänt intresse ska stå i proportion till det eftersträvade syftet samt vara förenligt med det väsentliga innehållet i rätten till dataskydd. Enligt skäl 4 till förordningen bör behandlingen av personuppgifter utformas så att den tjänar människor. Rätten till skydd för personuppgifter är inte en absolut rättighet utan den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen (jfr EU-domstolens avgörande i mål C-439/19, *Latvijas Republikas Saeima*, punkt 105).

I vissa situationer kan det framstå som givet att proportionalitetsprincipen inte är uppfylld och att en åtgärd är alldeles för ingripande för att vara godtagbar. I andra fall är det tvärtom så att det står klart att proportionalitetsprincipen är uppfylld. I många situationer är det dock svårt att utan närmare överväganden konstatera om en åtgärd är proportionerlig eller inte, och det kan beroende på omständigheterna finnas ett relativt stort bedömningsutrymme.

[3] Se Danelius, Danelius, Bull och Cameron, *Mänskliga rättigheter i europeisk praxis, En kommentar till Europakonventionen om de mänskliga rättigheterna* (version 6 JUNO, 2023), s. 65.

17.4 Faktorer till men för den personliga integriteten

Ett flertal olika faktorer påverkar hur allvarlig inskränkningen av rättigheter, som verksamheten med ett identitetsindex medför, sammantaget kan anses vara. Vi redogör i detta avsnitt för faktorer som är till men för den personliga integriteten. I nästa avsnitt belyser vi de omständigheter som vi anser minskar integritetsintrånget.

17.4.1 Ett stort antal personer skulle komma att omfattas

Verksamheten med ett identitetsindex kan komma att omfatta ett mycket stort antal personer. I tabellen nedan ges en översikt av antalet ärenden per år i de ärendeslag – eller liknande ärendeslag – där en identitetsnyckel bör kunna skapas.

Tabell 17.1 Antal ärenden per år

Ärendeslag	2022	2023	2024
Pass	2 586 135	1 591 928	1 686 245
Nationellt identitetskort	1 020 265	527 685	601 180
Beviljade UT (första)	135 189	97 129	88 956
Flyttning till Sverige	105 287	107 375	144 146
Ändring av id-uppgift	4 215	5 197	7 182
Ansökan om förnyelse av samordningsnummer	5 370	10 564	10 670
Enskilds ansökan om samordningsnummer	22 123	18 386	22 984
Naturalisation, avgjorda	74 086	58 541	55 725
Totalt	**3 952 670**	**2 416 805**	**2 617 088**

Det är utifrån denna statistik svårt att dra några säkra slutsatser kring det totala antalet ärenden där en identitetsnyckel bör kunna skapas, inte minst med hänsyn till att antalet ärenden varierar betydligt från år till år, och att vissa ärendeslag – utfärdande av statligt identitetskort och statlig e-legitimation – bygger på att lämnade författningsförslag genomförs. Det kan också vara så att samma person förekommer i mer än ett aktuellt ärendeslag; en person kan till exempel beviljas både ett pass och ett statligt identitetskort. Även med beaktande av detta anser vi att en försiktig bedömning ger vid handen

att ett identitetsindex årligen skulle kunna komma att tillföras ansiktsbilder och biometriska uppgifter som tas fram ur dessa från i vart fall två miljoner personer, inledningsvis främst i samband med att en identitetsnyckel skapas och därefter även i samband med uppdatering av uppgifter. I denna personkrets kommer, enligt våra överväganden i kapitel 12, såväl svenska medborgare som EES-medborgare och tredjelandsmedborgare att ingå. Att biometriska uppgifter behandlas för en stor mängd personer är en omständighet som särskilt måste beaktas. Att så få uppgifter som möjligt ska samlas in och behandlas är en grundläggande princip enligt artikel 5.1 c i dataskyddsförordningen. Av skäl 75 till förordningen framgår att risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling, bland annat om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade. EU-domstolen har i mål C-205/21, *V.S mot Ministerstvo na vatreshnite raboti m.fl.*, som visserligen avsåg det så kallade brottsdatadirektivet, uttalat bland annat att behovet av att behandla känsliga uppgifter ska bedömas med särskilt iakttagande av principen om uppgiftsminimering (punkt 125). Detta gäller som vi ser det även vid integritetsintrång som hänför sig till behandling av personuppgifter enligt dataskyddsförordningen.

Att biometriska uppgifter för ett mycket stort antal personer kan komma att behandlas i verksamheten med ett identitetsindex är enligt vår mening därmed en omständighet som negativt påverkar intrånget i den personliga integriteten och privatlivet. Som vi återkommer till i avsnitt 17.4.1 är personkretsen emellertid noga avgränsad utifrån syftet med verksamheten med ett identitetsindex, vilket talar i motsatt riktning.

17.4.2 Uppgifter om barn kommer att behandlas

En särskild omständighet att beakta är att ansiktsbilder och biometriska uppgifter som tas fram ur dessa som är kopplade till barn skulle behöva behandlas i verksamheten med ett identitetsindex. Enligt FN:s konvention om barnets rättigheter (barnkonventionen) ska det vid alla åtgärder beaktas vad som bedöms vara barnets bästa. Inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privatliv. När det gäller skapandet av en identitetsnyckel och

uppdatering av uppgifter kopplade till den i ett index kommer det enligt våra bedömningar i kapitel 13 och 14 att ske i samband med åtgärder i ett annat ärende, där biometriska underlag redan har tagits upp. Vi anser i övrigt – i likhet med den bedömning som gjordes i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* – att det är svårt att se att integritetsintrånget skulle vara större för ett barn än för en vuxen person, vilket har bäring även vid behandlingen av biometriska uppgifter i verksamheten med ett identitetsindex.[4]

17.4.3 Utökad upptagning av biometriska underlag

Som vi redogjort för i kapitel 13 kommer biometriska underlag inte att tas upp enbart i syfte att en identitetsnyckel ska kunna skapas utan detta skulle ske i samband med att Polismyndigheten, Migrationsverket eller Skatteverket tar upp biometriska underlag i samband med handläggningen av vissa typer av ärenden. Upptagningen av biometriska underlag skulle som sådan därmed inte medföra ett ytterligare intrång i integriteten för den enskilde i denna del av verksamheten. Detsamma bör gälla vid uppdatering av biometriska uppgifter i ett index.

Vid rättelse av biometriska uppgifter kan det däremot vara nödvändigt att på nytt ta upp biometriska underlag, vilket i så fall skulle medföra en utökad upptagning av ansiktsbilder (se avsnitt 14.4). Vad gäller upptagning av biometriska underlag har EU-domstolen emellertid uttalat att utöver att insamling av tio fingeravtryck och en ansiktsbild gör det möjligt att på ett tillförlitligt sätt identifiera den berörda personen, innebär insamlingen inte något ingrepp i intimsfären och medför inte heller något större fysiskt eller psykiskt obehag för personen (mål C-70/18, *Staatsecretaris van Justitie en Veiligheid mot A m.fl.*, punkt 58). Den utökade upptagning av biometriska underlag som verksamheten med ett identitetsindex skulle medföra bör enligt vår mening därför inte anses utgöra någon mer betydande integritetsinskränkning.

Vid verifiering av identitet på förfrågan av de aktörer som vi bedömer bör få kontrollera uppgifter mot ett index kommer biometriska underlag också att behöva tas upp. Vi återkommer till detta i kapitel 21.

[4] SOU 2025:75, s. 431 f.

17.4.4 Utökad lagring av biometriska uppgifter

Lagring av biometriska uppgifter utgör i sig en risk för integritetsintrång, bland annat med hänsyn till att det alltid finns en risk för att uppgifterna – trots rättsliga och tekniska skyddsåtgärder – blir tillgängliga för obehöriga, som kan använda uppgifterna i andra sammanhang utan den enskildes kännedom eller samtycke. Som pekades på i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* skulle en ansiktsbild med tillhörande biometriska uppgifter kunna användas inte bara för identifikation utan också för att ta del av eller kartlägga enskilda personers yttre kännetecken, såsom hudfärg eller etnicitet, i syften som går utöver det avsedda. Lagring av en ansiktsbild av en person kan vidare i sig vara integritetskränkande för en person som av religiös övertygelse eller annat skäl täcker sitt ansikte eller inte vill låta fotografera sig.[5]

Vid skapandet av en identitetsnyckel kommer biometriska uppgifter och andra personuppgifter att lagras i ett identitetsindex, utöver den lagring som kan ske i det aktuella ärendeslaget i något av de befintliga register som förs av Polismyndigheten, Migrationsverket eller Skatteverket (se avsnitt 10.3.2 för en översikt). Detta är fallet om en identitetsnyckel skapas när ett uppehållstillståndskort med en giltighetstid om mer än ett år utfärdas. Biometriska uppgifter avseende den utländska medborgaren kommer då även att lagras i Migrationsverkets register under viss tid, i enlighet med nuvarande och föreslagna bestämmelser.[6] Detsamma gäller om en identitetsnyckel skapas i samband med utfärdande av pass, statligt identitetskort eller statlig e-legitimation; en ansiktsbild och biometriska uppgifter ur den ska då lagras i det nuvarande passregistret eller det föreslagna pass- och identitetskortsregistret eller den föreslagna databasen över statliga e-legitimationer.[7]

I andra situationer kan det vara så att biometriska uppgifter kommer att lagras i ett identitetsindex men inte i ett annat befintligt, eller föreslaget, register. En identitetsnyckel bör enligt vår bedömning exempelvis kunna skapas i samband med ett medborgarskapsärende, oavsett utgång (se avsnitt 13.3.1). När ett svenskt medborgarskap

[5] SOU 2025:75, s. 430.
[6] Se förslag till ny lydelse av 15 § utlänningsdatalagen (2016:27) i *Stärkt återvändandeverksamhet*, prop. 2025/26:263, s. 182 f. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.
[7] Promemorian *Ett statligt identitetskort* (Ju202601595), s. 130 och 139 och *En statlig e-legitimation*, prop. 2025/26:250, s. 57.

beviljas ska de hos Migrationsverket tidigare lagrade biometriska uppgifterna emellertid gallras.[8] Det innebär att det endast är när medborgarskap *inte* beviljas som de biometriska uppgifter som tagits fram i ärendet skulle lagras både i ett identitetsindex och i Migrationsverkets register. Det är emellertid rimligt att anta att den som beviljas svenskt medborgarskap kommer att ansöka om svenskt pass eller ett statligt identitetskort och i samband med det kommer ansiktsbild och biometriska uppgifter från den att lagras, i enlighet med föreslagna bestämmelser, i andra register än ett identitetsindex.

Vidare kan vi konstatera att Skatteverket får, och enligt lämnade förslag ska få, ta upp biometriska underlag vid identitetskontroll enligt folkbokföringslagen (1991:481) och lagen (2022:1697) om samordningsnummer. Fingeravtryck, ansiktsbilder och biometriska uppgifter som tas fram ur dessa får behandlas i folkbokföringsverksamheten med stöd av bestämmelserna i 5 och 8 §§ folkbokföringsdatalagen (2026:126) och enligt 1 a § folkbokföringslagen, i dess lydelse från och med den 1 december 2026, ska Skatteverket registrera biometriska underlag och biometriska uppgifter om en person. Det kan dock vara så att endast fingeravtryck tas upp och lagras, om Skatteverket bedömer att den enskildes identitet kan kontrolleras tillfredsställande genom upptag av endast denna typ av underlag.[9] Det är alltså inte säkert att de biometriska uppgifter som har tagits fram i ärendet kommer att lagras både i folkbokföringsverksamheten och i identitetsindexet i dessa fall.

Även om biometriska uppgifter i majoriteten av fallen alltså kommer att lagras även i andra register kommer ett identitetsindex att innebära en utökad lagring av sådana uppgifter, med de särskilda risker som detta kan innebära och som vi pekat på ovan. Vidare kan vi konstatera att integritetsintrånget kommer att variera utifrån personkrets. Ett identitetsindex skulle, enligt våra överväganden i kapitel 12 och 13, kunna komma att innehålla biometriska uppgifter från såväl svenska medborgare som EES-medborgare och tredjelandsmedborgare, medan exempelvis passregistret endast innehåller uppgifter om svenska medborgare och Migrationsverkets register endast uppgifter om utländska medborgare. Det föreslagna pass- och iden-

[8] Se 3 § utlänningsdataförordningen (2016:30).
[9] SOU 2025:75 s. 565 f.

titetskortsregistret kommer däremot att innehålla uppgifter såväl om svenska medborgare som vissa utlänningar.[10]

17.4.5 Utökad behandling av biometriska uppgifter

Såväl att ta upp biometriska underlag som att lagra dessa och de biometriska uppgifter som kan tas fram ur dem utgör, enligt artikel 4.2 i dataskyddsförordningen, behandling av personuppgifter. Dessa två sätt att behandla personuppgifter är grundläggande för att en identitetsnyckel ska kunna skapas. I den verksamhet med ett identitetsindex som innebär verifiering av identitet efter en begäran av någon av de aktörer som vi anser bör få använda ett index på detta sätt (se kapitel 21), kommer biometriska underlag och/eller uppgifter också att behöva behandlas. Detsamma gäller vid uppdatering, rättelse och radering av uppgifter i ett identitetindex, på det sätt som vi redogjort för i kapitel 14 och 15. Med hänsyn till detta och utifrån att vi i de föregående avsnitten har bedömt att verksamheten med ett identitetsindex medför en utökad upptagning av biometriska underlag och en utökad lagring av biometriska uppgifter står det klart att verksamheteten kommer att innebära en utökad behandling av biometriska uppgifter. Till detta kommer den behandling av biometriska uppgifter som eventuellt kan behöva utföras av den aktör som vill använda ett index för att verifiera identitet med hjälp av sådana uppgifter i ett visst enskilt fall. Vi tar i avsnitt 18.3.3 ställning till detta.

17.4.6 Begränsade möjligheter att undvika en registrering

Den som vänder sig till Polismyndigheten, Migrationsverket eller Skatteverket i något av de ärendeslag som vi anser bör kunna leda till att en identitetsnyckel skapas för den enskilde ska – i enlighet med artikel 13 i dataskyddsförordningen – informeras om att de biometriska underlag som tas upp och övriga personuppgifter som samlas in kan komma att användas även i detta syfte. Den enskilde har därmed en möjlighet att utifrån den informationen välja att inte lämna biometriska underlag. Detta kan dock få till följd att den enskilde får ett negativt beslut, till exempel att pass inte kan utfärdas eller att ett samordningsnummer på styrkt identitetsnivå inte kan

[10] Se promemorian *Ett statligt identitetskort*, Ju2026/01595, s. 59 och 130.

tilldelas. Vi kan vidare konstatera att en identitetsbeteckning, särskilt personnummer, i praktiken fungerar som en nyckel för att kunna delta i samhället. Detta talar tydligt mot att den enskilde kan avstå från att inleda ett sådant ärende för att undvika att en identitetsnyckel skapas. Innehav av pass eller nationellt identitetskort – alternativt statligt identitetskort med resefunktion – är för svenska medborgare vidare en förutsättning för att kunna resa och utnyttja rätten till fri rörlighet inom unionen. Det kan därför med fog hävdas att det i praktiken inte finns något egentligt val för den enskilde gällande registrering i ett identitetsindex; om han eller hon vill ha till exempel ett pass eller ett samordningsnummer på styrkt identitetsnivå skulle det – om ett system med ett index införs – som utgångspunkt inte gå att undvika att en identitetsnyckel samtidigt skapas.

En gemensam nämnare för de ärendeslag som vi enligt våra överväganden i kapitel 13 anser bör kunna leda till att en identitetsnyckel skapas är att det är fråga om att i någon form stärka eller bibehålla en koppling till Sverige. De personer som aktualiseras i ärendena vill få rätt att vistas i Sverige, flytta till Sverige, bli svenska medborgare eller få en rese- eller identitetshandling utfärdad av svenska myndigheter. Vad gäller samordningsnummer kan tilldelning ha begärts antingen av den enskilde eller av en myndighet. För att en identitetsnyckel ska kunna skapas i samband med tilldelning av samordningsnummer måste den enskilde inställa sig personligen och biometriska underlag tas upp. Om samordningsnummer tilldelas på begäran av en myndighet och den enskilde inte inställer sig personligen kommer en registrering i ett identitetsindex inte att kunna göras även om samordningsnummer tilldelas, eftersom biometriska underlag i sådant fall inte har kunnat tas upp. Den enskilde har alltså vid tilldelning av samordningsnummer på begäran av en myndighet en viss möjlighet att förhindra att en identitetsnyckel då skapas för honom eller henne. Även med hänsyn till detta anser vi att en person som vill bli folkbokförd, tilldelas ett samordningsnummer eller få ett sådant nummer förnyat, vill få rätt att vistas i Sverige, vill bli svensk medborgare eller vill få ett pass eller en identitetshandling utfärdad av svenska myndigheter, i princip inte kommer att ha någon möjlighet att avstå från att bli registrerad i ett identitetsindex.

17.5 Faktorer som minskar integritetsintrånget

De faktorer som vi redogjort för i föregående avsnitt är av sådan karaktär att de inskränker skyddet för den personliga integriteten och rätten till privatliv på olika sätt. Vi kan samtidigt konstatera att verksamheten med ett identitetsindex, om ett index införs, även skulle komma att innehålla faktorer som verkar i motsatt riktning.

17.5.1 En avgränsad personkrets, utifrån syftet med ett index, och ett tydligt behov

Som vi konstaterat i avsnitt 17.3.1 kan verksamheten med ett identitetsindex komma att omfatta såväl svenska som utländska medborgare (EES-medborgare och tredjelandsmedborgare). En identitetsnyckel bör dock inte kunna skapas för samtliga personer som tillhör dessa kategorier. För det första har vi i kapitel 12 bedömt att det endast är de personer som har en viss anknytning till Sverige som bör kunna ingå i ett identitetsindex, på grund av hemvist, bosättning eller annan anknytning till landet. Generellt sett bör personer som vistas endast tillfälligt i landet inte omfattas. Vissa kategorier av personer bör också helt undantas, bland annat barn som inte har fyllt sex år. I kapitel 13 har vi ytterligare begränsat personkretsen genom att en identitetsnyckel bör skapas för en person endast i vissa ärendeslag och under vissa förutsättningar. Sammantaget innebär detta att endast de personer vars identitet kan antas behöva verifieras i olika sammanhang – i första hand under vistelse i landet – kommer att ingå i ett identitetsindex, och att en identitetsnyckel endast kommer att skapas för de personer som kommer i kontakt med Polismyndigheten, Migrationsverket och Skatteverket i vissa ärendeslag. Att personkretsen på detta sätt blir avgränsad genom en direkt koppling till syftet med identitetsindexet skiljer sig, som vi ser det, från både folkbokföringsverksamheten och den centrala utlänningsdatabasen. Dessa register saknar en motsvarande direkt koppling, då den information som behandlas i dessa register kan användas i många olika ärendeslag; uppgifterna i folkbokföringen ligger exempelvis till grund för många andra myndigheters information om enskilda.

När det gäller behovet av att behandla personuppgifter i verksamheten med ett identitetsindex för de olika kategorier av medborgare som enligt vår bedömning bör kunna omfattas kan – utöver vad som

anförts i kapitel 12 – vissa särskilda omständigheter beaktas i ljuset av en proportionalitetsbedömning; ett mycket tydligt behov av att, utifrån syftet med ett identitetsindex, behandla personuppgifter för en viss kategori personer bör som vi ser det vara en tydlig indikation på att behandlingen också är proportionerlig. Vi anser – på de skäl som anförs nedan – att om verksamheten med ett identitetsindex som sådan är proportionerlig, är det även proportionerligt att i verksamheten behandla personuppgifter för såväl svenska medborgare som utländska medborgare (EES-medborgare och tredjelandsmedborgare) och statslösa.

Särskilt om svenska medborgare

Det är enligt vår bedömning inte orimligt att anta att möjligheten att använda ett identitetsindex för kontroll av identitet kommer att användas mer begränsat avseende svenska medborgare än för tredjelandsmedborgare och EES-medborgare. Svenska medborgare som är födda i landet registreras i folkbokföringen direkt vid födseln och identiteten är då i normalfallet styrkt. Svenska medborgare har också i större utsträckning godtagbara identitetshandlingar som är utfärdade av svenska myndigheter, och därmed är vanligt förekommande och väl kända för de myndigheter och andra aktörer som kan behöva verifiera identitet. Integritetsintrånget för många svenska medborgare kommer därför huvudsakligen att bestå i att personuppgifter om dem behandlas i verksamheten med ett identitetsindex i samband med att en identitetsnyckel skapas eller när uppgifterna löpande behöver uppdateras på det sätt som vi redogjort för i avsnitt 14.3.

Att det kan finnas ett mer begränsat behov av att verifiera identitet för svenska medborgare genom kontroll av biometriska uppgifter skulle kunna ses som ett argument mot att denna personkategori bör registreras i ett index. Verksamheten med ett identitetsindex syftar emellertid inte endast till att vara en kontrollfunktion för myndigheter utan har en skyddsfunktion för enskilda, genom att det motverkar att identiteter utnyttjas av andra. Just med hänsyn till att svenska medborgares identitet sällan ifrågasätts kan det finnas ett större incitament att utnyttja svenska medborgares identitet. Behovet av att denna personkategori ingår i ett identitetsindex kan därför, enligt vår mening, inte sägas vara mindre än för EES-med-

borgare eller tredjelandsmedborgare, och är en omständighet som är viktig att beakta. Syftet att skydda enskilda svarar också direkt mot det som framgår av artikel 52.1 i EU:s rättighetsstadga, det vill säga att en begränsning av rätten till skydd för privatlivet får göras om den svarar mot behovet av skydd för andra människors rättigheter och friheter. Vi anser vidare att om ett system med ett identitetsindex införs bör det omfatta en så stor andel som möjligt av de personer som vistas i Sverige eller av annan anledning kan antas komma i kontakt med svenska myndigheter regelbundet, för att det effektivt ska kunna fylla avsedd funktion.

Särskilt om EES-medborgare

Det har i andra sammanhang konstaterats att utnyttjade och kapade identiteter används för identitetsmissbruk (se kapitel 9). Ett upplägg som förekommer är att EES-medborgare som kan utnyttja rätten till fri rörlighet inom unionen hämtas till Sverige i syfte att registreras i folkbokföringen för att få ett person- eller samordningsnummer som kan användas på många olika sätt. EES-medborgaren vistas endast tillfälligt i Sverige för att genomgå identitetskontroll vid ett personligt besök på ett servicekontor i samband med anmälan om flyttning i Sverige, och för att få fysiska och digitala identitetshandlingar utfärdade. En sådan så kallad skeninvandring kan ligga till grund för att andra personer sedan utnyttjar EES-medborgarens identitet när denne återvänt till sitt hemland.[11] Denna form av upplägg underlättas av att EES-medborgare inte behöver uppehållstillstånd för att vistas i Sverige utan kan vistas här med uppehållsrätt. En tredjelandsmedborgare har inte motsvarande möjlighet till fri rörlighet. Det kan därför antas att denna form av skeninvandring, som görs endast i syfte att utnyttja en persons identitet, är betydligt vanligare för EES-medborgare än för tredjelandsmedborgare. Detta stöds även av Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter*; Riksrevisionen uttalade att bedrägerier kopplade till verifieringen av identitet hos personer som invandrat från EES har beskrivits

[11] Jfr *Folkbokföringsverksamhet, biometri och brottsbekämpning,* SOU 2025:75, s. 283 f. och 415, *Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen,* SOU 2020:35, s. 144, *Intyget som dörröppnare till välfärdssystemet,* Rapport 2015:8, Brå, s. 82 f. och Skatteverkets redovisning av regeringsuppdrag att inrätta ett pilotprojekt för att komma åt felaktig folkbokföring kopplad till organiserad brottslighet, dnr 8-1245868, 2021-10-01, s. 6.

som en riskfaktor och att omfattningen av de förmåner som betalas ut till EES-medborgare uppgick till närmare 115 miljarder kronor för åren 2011–2021. Även om endast en mindre andel av dessa utbetalningar skulle ske på felaktig grund kopplat till utnyttjande av identitet rör det sig, enligt Riksrevisionen, om betydande belopp.[12]

Dessa omständigheter visar enligt vår mening på ett tydligt behov av att kunna behandla personuppgifter för EES-medborgare i verksamheten med ett identitetsindex, för att kunna verifiera identitet för dessa med grund i biometriska uppgifter. Vi kan i detta sammanhang konstatera att i betänkandet *Registrering av EES-medborgare* har förslag lämnats om att EES-medborgare som vistas i Sverige i över tre månader som huvudregel ska vara registreringsskyldiga. Enligt förslagen ska Migrationsverket ha möjlighet att ta fotografi och fingeravtryck i ärenden om registrering av uppehållsrätt och att ta fram biometriska uppgifter ur dessa, för att kontrollera identitet mot uppgifterna i EES-medborgarens pass eller identitetskort.[13] Även om sådana åtgärder kan främja en utökad kontroll av EES-medborgares vistelse i Sverige bedömer vi att en registrering av EES-medborgare även i ett identitetsindex kan främja att multipla identiteter upptäcks. Vi kan i detta sammanhang även notera att experter från Skatteverket, i ett särskilt yttrande till betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* bedömde att det är tydligt att behovet av lagring och användning av en persons biometriska underlag och de biometriska uppgifter som kan tas fram ur dessa är minst lika framträdande avseende personer som uppger sig vara EES-medborgare som för personer som uppger sig vara medborgare i tredje land.[14]

En särskild fråga är om rätten till fri rörlighet medför att behandlingen av biometriska uppgifter för EES-medborgare i ett register är att anse som oproportionerlig. Denna fråga belystes, avseende Skatteverkets möjligheter att lagra sådana uppgifter, i nyss nämnda betänkande. Enligt förslag i betänkandet skulle biometriska underlag och uppgifter för EES-medborgare få lagras endast om det finns anledning att anta att personen vid en identitetskontroll lämnar eller har lämnat oriktiga uppgifter. Utredningen lade vid sin bedömning vikt vid ett yttrande från europeiska datatillsynsmannen den 13 september 2024

[12] RiR 2024:12, s. 9.
[13] SOU 2026:9, s. 119 och 194 ff.
[14] SOU 2025:75, s. 596.

avseende förslag om ny förordning om säkrare identitetskort för unionsmedborgare och en uppgift från Integritetsskyddsmyndigheten om att det, såvitt myndigheten känner till, inte i någon annan medlemsstat finns en ordning som motsvarar den som var föremål för utvärdering, samt i viss mån EU-domstolens praxis avseende omfattande och odifferentierad lagring avseende andra typer av uppgifter på andra områden.[15]

Vi anser att de omständigheter som lyftes fram i nämnda betänkande inte innebär att det är oproportionerligt att behandla biometriska uppgifter för EES-medborgare i verksamheten med ett identitetsindex, av följande skäl. Vi kan för det första konstatera att nyss nämnda id-kortsförordning[16] – som ersatts av en ny förordning[17] – avser möjlighet att lagra fingeravtryck i fysiska identitetshandlingar. Det framstår därför som naturligt att det eftersträvade målet med den regleringen inte kan motivera lagring i register av biometriska uppgifter för upp till 370 miljoner personer (se EU-domstolens dom i mål C-61/22, *RL mot Landeshauptstadt Wiesbaden*, punkt 35). Verksamheten med ett identitetsindex rör ett annat sakområde och har ett annat syfte. Omfattningen av antalet berörda personer är visserligen stor, men enligt vår mening inte jämförbar. Vad som uttalats i ovan nämnda yttrande från europeiska datatillsynsmannen har därför – enligt vår mening – inte någon direkt bäring på proportionalitetsbedömningen i det nu aktuella sammanhanget. Vad gäller argumentet att ingen annan medlemsstat har ett system liknande ett identitetsindex säger detta i sig inte något om huruvida ett sådant system är lämpligt eller rättsligt genomförbart i Sverige. För det fall EU-domstolen hade underkänt ett liknande system hade det naturligtvis varit relevant för våra överväganden. Det hade även varit relevant om ett liknande system utretts och avfärdats som oförenligt med grundläggande rättigheter eller dataskyddsförordningen av någon annan medlemsstat. Såvitt vi känner till har ett liknande system dock varken prövats av EU-domstolen eller utretts av en annan medlemsstat.

Det finns alltså enligt vår mening ett mycket tydligt behov av att behandla biometriska uppgifter för EES-medborgare i verksamheten med ett identitetsindex och det saknas, enligt vår bedömning, några

[15] SOU 2025:75, s. 454.
[16] Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019.
[17] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.

särskilda omständigheter som medför att det skulle vara oproportionerligt att behandla uppgifter just för EES-medborgare. Vi kan dessutom här konstatera att regeringen, i propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* anförde bland annat att det är avgörande att även EES-medborgares biometriska uppgifter kan sparas för att motverka identitetsmissbruk och dess användning för välfärdsbrott och inom organiserad brottslighet. Regeringen ansåg därför – till skillnad från vad som anfördes i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* – att någon begränsning i fråga om lagring i folkbokföringsverksamheten av uppgifter för EES-medborgare inte ska gälla.[18] Det kan även beaktas att vi i kapitel 12 har bedömt att en identitetsnyckel i första hand bör kunna skapas för en EES-medborgare när denne folkbokförs eller tilldelas ett samordningsnummer, det vill säga vid en tidpunkt då den form av upplägg som beskrivits ovan möjliggörs. Detta begränsar enligt vår mening kretsen av EES-medborgare på ett proportionerligt sätt.

Särskilt om tredjelandsmedborgare

Vår bedömning är att behovet, generellt sett, av att kunna verifiera identitet för tredjelandsmedborgare inte kan antas vara mindre än för EES-medborgare och svenska medborgare. Detta beror bland annat på att de i högre utsträckning än de två övriga grupperna kan sakna godtagbara identitetshandlingar, och att de inte på samma sätt som svenska medborgare är kända för svenska myndigheter sedan en längre tid. De kan också ha beviljats uppehållstillstånd i Sverige utan att identiteten har styrkts, exempelvis när uppehållstillståndet grundar sig på ett skyddsbehov eller familjeåterförening. Det finns därmed också en större risk för att en tredjelandsmedborgare uppträder under multipla identiteter, vilket verksamheten med ett identitetsindex bland annat syftar till att motverka.

Det finns, enligt vår bedömning, inte några särskilda omständigheter hänförliga till just tredjelandsmedborgare som medför att det skulle vara oproportionerligt att behandla biometriska uppgifter och andra personuppgifter om dem i verksamheten med ett index. I detta sammanhang kan vi konstatera att när det gäller tredjelandsmedborg-

[18] Prop. 2025/26:261, s. 48.

are har det på EU-nivå under senare år genomförts flera lagstiftningsåtgärder som bland annat syftar till att motverka identitetsmissbruk och där en del av dessa åtgärder innefattar lagring och behandling av biometriska uppgifter för tredjelandsmedborgare. De EU-gemensamma informationssystemen kan antas komma att omfatta betydligt fler personer än verksamheten med ett identitetsindex, och ska kunna användas av myndigheter i alla medlemsstater. Något som tyder på att den behandlingen är att betrakta som oproportionerlig eller oförenlig med grundläggande rättigheter har inte kommit fram. I propositionen *Anpassning av svensk rätt till EU:s nya in- och utresesystem* konstaterade regeringen – med anledning av att en mer utförlig proportionalitetsbedömning hade efterfrågats av vissa remissinstanser – bland annat att EU:s regelverk, däribland in- och utreseförordningen[19], om den enskildes lämnande och myndigheternas användning av fingeravtryck och andra personuppgifter är omgärdat av detaljerade bestämmelser som syftar till att skydda den enskilde.[20] Vi kan notera att det framgår av skäl 59 till in- och utreseförordningen att förordningen bedöms förenlig med de grundläggande rättigheter och principer som erkänns i EU:s rättighetsstadga.[21]

17.5.2 En begränsad uppsättning uppgifter

Vår bedömning

Ett identitetsindex kommer att innehålla endast de uppgifter som är nödvändiga för att en identifiering eller en verifiering av identitet ska kunna genomföras.

Vi har i kapitel 11 redogjort för vilka typer av uppgifter som vi anser är nödvändiga för att syftet med ett identitetsindex ska kunna uppnås. Behandling av personuppgifter i verksamheteten med ett identitetsindex som utförs med stöd av den rättsliga grunden uppgift av allmänt intresse i artikel 6.1 e i dataskyddsförordningen ska vara nödvändig. I detta krav ligger bland annat att principen om uppgiftsminimering enligt artikel 5.1 c ska beaktas. För att en utökad behandling av uppgifter i verksamheten med ett identitetsindex ska vara

[19] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.
[20] Prop. 2021/22:81, s. 19.
[21] Se även skäl 47 till in- och utreseförordningen.

förenlig med dataskyddsförordningen bör alltså mängden personuppgifter som behandlas begränsas till vad som är nödvändigt för att uppnå ändamålen med behandlingen. Ett index ska alltså inte innehålla fler uppgifter än vad som är nödvändigt. Vi gör i detta avseende följande överväganden.

Verksamheten med ett identitetsindex bör enligt vår bedömning i avsnitt 10.7.6 byggas upp från grunden, genom att en identitetsnyckel skapas i vissa situationer, och att vissa uppräknade uppgifter då kopplas till nyckeln i systemet. Ett identitetsindex är tänkt att existera separerat från befintliga register som förs av Polismyndigheten, Migrationsverket och Skatteverket. Dessa register innehåller i varierande utsträckning dels biometriska underlag och biometriska uppgifter, dels andra personuppgifter som är relevanta för den specifika verksamheten. Genom en separering av verksamheten med ett identitetsindex från befintliga register kommer ett index inte att innehålla andra uppgifter än de som är nödvändiga för just det syfte som verksamheten ska uppnå, det vill säga, i första hand, verifiering av identitet. Det begränsar riskerna med behandling av personuppgifterna och det integritetsintrång som den medför.

I enlighet med våra bedömningar i kapitel 11 skulle ett identitetsindex innehålla följande alfanumeriska uppgifter, när dessa är tillgängliga: namn, födelsetid, medborgarskap, personnummer eller samordningsnummer och Migrationsverkets individnummer. Enligt vår bedömning i avsnitt 11.4.5 bör inte fingeravtryck eller biometriska uppgifter som kan tas fram ur dem få lagras i ett index. Däremot är ansiktsbilder och biometriska uppgifter som tas fram ur dem nödvändiga för att syftet med ett identitetsindex ska kunna uppnås. Biometriska uppgifter ur ansiktsbilder är i den stora majoriteten fall tillräckliga för att identitet ska kunna verifieras på ett tillräckligt säkert sätt när ett behov av verifiering aktualiseras. Tekniken för ansiktsigenkänning baseras på en uppskattad matchning mellan olika mallar, där jämförelsen leder till en högre eller lägre sannolikhet för att personen verkligen är den person var identitet ska verifieras. Om sannolikheten överstiger ett visst tröskelvärde i systemet kommer det att visa en träff.[22] För det fall en tillräcklig grad av sannolikhet inte uppnås och ett identitetsindex därmed inte genererar en träff ankommer det på den myndighet som har behov av att verifiera en

[22] Riktlinjer 05/2022 om användningen av teknik för ansiktsigenkänning på brottsbekämpningsområdet, version 2.0, den 26 april 2023, punkt 11.

persons identitet att utifrån övriga omständigheter ta ställning till hur det aktuella ärendet fortsatt ska hanteras.

Jämfört med exempelvis folkbokföringsverksamheten är det alltså fråga om en mycket begränsad uppsättning personuppgifter som behöver behandlas i verksamheten med ett identitetsindex. Detta påverkar integritetsintrångets allvar. I betänkandet *Personuppgifter och mediegrundlagarna* anfördes bland annat, avseende offentliggörande av personuppgifter genom söktjänster, att även om varje uppgift i sig inte är integritetskänslig kan uppgifterna sammantaget ge en översikt av en enskilds personliga förhållanden som blir problematisk ur integritetssynpunkt, och att så kan vara fallet exempelvis om det i en uppgiftssamling går att söka på namn eller personnummer och därigenom få uppgift om personens adress, ålder och inkomst.[23] I propositionen *Samverkan mot penningtvätt och finansiering av terrorism* anförde regeringen att även ett utbyte av förhållandevis harmlösa uppgifter riskerar att leda till integritetsintrång om de skapar en tydligare bild av en enskilds personliga förhållanden.[24] Vi anser att dessa uttalanden gör sig gällande även vid behandling av personuppgifter i ett register. Ett identitetsindex kommer dock, om det införs, inte att innehålla uppgifter som medger någon kartläggning av en individ på det sätt som pekats på i nämnda förarbeten.

Som vi återkommer till i avsnitt 17.4.3 bedömer vi att de uppgifter som behöver behandlas som utgångspunkt inte heller – förutom vad gäller ansiktsbild och de biometriska uppgifter som kan tas fram ur den – är av känslig art. Uppgifterna kommer som utgångspunkt dessutom att behandlas även i något av de befintliga register som förs av Skatteverket, Migrationsverket eller Polismyndigheten.

17.5.3 Personuppgifternas karaktär

Vår bedömning

Med undantag för biometriska underlag och biometriska uppgifter är de uppgifter som skulle behandlas i verksamheten med ett identitetsindex som utgångspunkt inte av känslig karaktär.

[23] *Personuppgifter och mediegrundlagarna*, SOU 2024:75, s. 196.
[24] Prop. 2021/22:251, s. 36.

I förarbetena till bestämmelsen i 2 kap. 6 § regeringsformen framhölls att det är naturligt att det läggs stor vikt vid personuppgifternas karaktär vid bedömningen av hur ingripande intrånget kan anses vara vid insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden; ju känsligare uppgifterna är, desto mer ingripande anses behandlingen av uppgifterna normalt vara.[25]

Att ansiktsbilder och biometriska uppgifter som kan tas fram ur dessa till sin natur är känsliga uppgifter står klart. När det gäller personnummer och samordningsnummer är de inte känsliga personuppgifter i dataskyddsförordningens mening, men har getts en särställning genom artikel 87, som anger att ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering endast får användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt förordningen. Vi bedömer att Migrationsverkets individnummer också utgör ett sådant identifikationsnummer som avses i bestämmelsen. Regeringen har i äldre förarbeten uttalat att själva personnumret inte i sig är en integritetskränkande uppgift, men att viss användning av det, såsom exempelvis samkörning av register och liknande kan uppfattas som integritetskränkande; ”onödig” användning ska betraktas som ett integritetsintrång.[26] Vi anser att dessa uttalanden gör sig gällande även för samordningsnummer och Migrationsverkets individnummer. Vi kan i detta sammanhang även notera att det i betänkandet *Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända* anfördes bland annat att ”den personuppgiftsbehandling som kommer att ske i enlighet med utredningens förslag [*i den arbetsmarknadspolitiska verksamheten, vår anmärkning*] rör i de flesta fall mindre känsliga uppgifter som namn, samordningsnummer, uppehållstillstånd och utbildning.”[27] Identitetsuppgifter, men även person-, samordnings- och individnummer, är dessutom uppgifter som enskilda regelmässigt på eget initiativ lämnar till myndigheter och andra aktörer i olika sammanhang, till exempel vid en ansökan om en förmån eller vid utlämnande av ett paket hos ett paketombud. Identitetsuppgifter – förutom medborgarskap – förekommer även öppet i många söktjänster på nätet.[28]

[25] *En reformerad grundlag*, prop. 2009/10:80, s. 183.
[26] Regeringens proposition 1990:91/60 om offentlighet, integritet och ADB, s. 69.
[27] SOU 2025:35, s. 317.
[28] SOU 2024:75, s. 142.

Det ovan anförda talar enligt vår mening mot att behandlingen av uppgifter om namn, födelsetid samt person-, samordnings- och individnummer i verksamheten med ett identitetsindex skulle utgöra en oproportionerlig inskränkning i de rättigheter som följer av regeringsformen, Europakonventionen och EU:s rättighetsstadga.

En indikation på hur känslig en viss typ av uppgift kan anses vara är vidare om den omfattas av sekretess, och i så fall vilket skaderekvisit som är tillämpligt. För uppgifter om den enskildes personliga förhållanden i folkbokföringsverksamheten råder det en presumtion för offentlighet. Sekretess gäller endast om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider med om uppgiften röjs. Undantaget är fotografisk bild av den enskilde, som skyddas av sekretess om det inte står klart att bilden kan röjas utan att den enskilde eller någon närstående till denne lider men. Detta framgår av 22 kap. 1 § offentlighets- och sekretesslagen (2009:400). Uppgift om namn, födelsetid och medborgarskap i folkbokföringsverksamheten är alltså vanligen offentliga liksom uppgift om person- och samordningsnummer. Motsvarande gäller enligt 6 § offentlighets- och sekretessförordningen (2009:641) för uppgifter om enskilds personliga förhållanden i passregistret, registret över nationella identitetskort och Skatteverkets databas över identitetskort för folkbokförda i Sverige. Enligt förslag i promemorian *Ett statligt identitetskort* ska samma sekretess gälla för pass- och identitetskortsregistret.[29] Även för databasen över statliga e-legitimationer ska motsvarande sekretess gälla, enligt förslag i propositionen *En statlig e-legitimation*.[30] Identitetsuppgifter skyddas dock av starkare sekretess när de förekommer i Migrationsverkets verksamhet än när de behandlas i folkbokföringsverksamheten; det råder då en presumtion för sekretess. I verksamhet för kontroll över utlänningar och i ärende om svenskt medborgarskap gäller enligt 37 kap. 1 § offentlighets- och sekretesslagen sekretess för uppgift om enskilds personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Beträffande beslut i ärenden gäller sekretessen dock endast för uppgifter i skälen. För uppgifter som rör en utlänning gäller dessutom, enligt 21 kap. 5 § offentlighets- och sekretesslagen, sekretess – oavsett i vilket sammanhang uppgiften förekommer – om det kan antas att röjande av upp-

[29] Ju2026/01595, s. 168 f.
[30] Prop. 2025/26:250, s. 65.

giften skulle medföra fara för att någon utsätts för övergrepp eller lider annat allvarligt men som föranleds av förhållandet mellan utlänningen och en utländsk stat eller myndighet eller organisation av utlänningar.

För huvuddelen av de personuppgifter som vi anser bör kunna få behandlas i verksamheten med ett identitetsindex råder alltså en presumtion för offentlighet hos den myndighet varifrån uppgifterna hämtas, när en identitetsnyckel skapas. Med hänsyn till detta och till vad vi ovan anfört angående karaktären på uppgifterna i sig bedömer vi att personuppgifterna – med undantag för ansiktsbild och de biometriska uppgifter som kan tas fram ur den – som utgångspunkt inte är av känslig karaktär. Inte heller sedda tillsammans anser vi att de kan anses vara av särskilt integritetskänslig karaktär, på de skäl som anförts i avsnitt 17.4.2.

17.5.4 Behandlingen av personuppgifter vid registrering, uppdatering, rättelse och radering är förutsebar

Vår bedömning

Det är tydligt för den enskilde när och under vilka förutsättningar en identitetsnyckel bör kunna skapas och vilka uppgifter om personen som då kan kopplas till nyckeln. Det är också förutsebart när uppgifter i verksamheten med ett identitetsindex kan komma att behöva uppdateras, rättas och raderas.

För att kravet på proportionalitet ska vara uppfyllt måste det enligt EU-domstolen föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden och minimikrav måste anges, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk.[31] Det innebär att en författning som ger stöd för behandling av personuppgifter i verksamheteten med ett identitetsindex måste vara förutsebar och formulerad på ett sådant sätt att enskilda kan anpassa sitt beteende efter den. Den måste skydda enskilda mot godtycklig tillämpning

[31] Se till exempel EU-domstolens dom i de förenade målen C-511/18, C-512/18 och C-520/18 *La Quadrature du Net m.fl.*, punkt 132.

och utrymmet för skönsmässig tillämpning måste vara tillräckligt tydligt avgränsat. Upptagningen av biometriska underlag vid skapandet av en identitetsnyckel och när uppgifter i verksamheten med ett identitetsindex bör uppdateras, rättas och raderas behöver regleras tydligt, så att det framgår från vem och under vilka förutsättningar insamling får ske samt vilka typer av biometriska underlag som får samlas in. Även behandlingen i övrigt av sådana uppgifter behöver ha stöd i en tydligt formulerad författning.

Vi anser att ett regelverk i fråga om verksamheten med ett identitetsindex, som utformas i enlighet med våra överväganden i kapitel 12–15 uppfyller dessa krav. De överväganden vi gjort i kapitel 13 gör det tydligt både för myndigheter och enskilda i vilka situationer en identitetsnyckel bör kunna skapas, och vilka biometriska underlag som då kan tas upp samt vilka andra uppgifter som behöver kopplas till identitetsnyckeln i samband med det. Såväl skapandet av en identitetsnyckel som den löpande uppdateringen av uppgifter i ett identitetsindex är knuten till vissa särskilda ärendeslag, vilket ökar förutsebarheten och tydligheten för både myndigheter och den enskilde. Även om rättelse av felaktiga alfanumeriska uppgifter i ett identitetsindex bör kunna göras på initiativ av myndigheten och utan den enskildes medverkan (se avsnitt 14.4) anser vi att det är tillräckligt tydligt när en sådan rättelse bör få göras, och hur den ska gå till. Vid rättelse av ansiktsbild och biometriska uppgifter kan det normalt sett förutsättas att den enskilde medverkar (se avsnitt 14.4.1). Den enskilde kan också välja att anpassa sitt beteende för att undvika att personuppgifter om honom eller henne behandlas i verksamheten med ett identitetsindex, även om det kan få andra konsekvenser som inte är önskvärda från den enskildes synvinkel, till exempel att han eller hon inte kan få ett pass utfärdat. Vidare saknas det i princip utrymme för skönsmässiga bedömningar vid ställningstagande till om och när en identitetsnyckel kan skapas eller uppgifter behöver kunna uppdateras löpande på det sätt vi beskrivit i avsnitt 14.3. Att verksamheten med ett identitetsindex, vid ett genomförande, skulle vara begränsad till ett fåtal myndigheter talar ytterligare för detta, och främjar som vi ser det också en förutsebarhet.

Sammantaget bedömer vi att behandlingen av personuppgifter i verksamheten med ett identitetsindex är tydlig och förutsebar, såväl vid skapandet av en identitetsnyckel som vid uppdatering, rättelse och radering av uppgifter.

17.5.5 Behandling skulle ske för huvudsakligen samma syften som i det ärendeslag som föranleder en registrering

Biometriska underlag tas primärt upp för att möjliggöra en identitetskontroll, exempelvis vid utfärdande av ett uppehållstillståndskort eller vid en ansökan om ett pass eller en annan identitetshandling. Även efter registrering av biometriska underlag och de biometriska uppgifter som kan tas fram ur dessa i ett identitetsindex kommer de att användas för att kontrollera identitet och motverka olika former av identitetsmissbruk. Verksamheten med ett identitetsindex har detta som primärt syfte. Ett identitetsindex bör, vilket vi återkommer till i avsnitt 18.2.1, inte kunna användas i till exempel den brottsbekämpande verksamheten, och även om det handlar om utökade möjligheter att kontrollera identitet kommer de biometriska uppgifterna – som utgångspunkt – inte att kunna användas till annat än just att säkerställa att en person som en aktör möter är den han eller hon utger sig för att vara. De personuppgifter – i synnerhet de biometriska underlagen och de biometriska uppgifter som kan tas fram ur dessa – som då skulle behandlas i verksamheten med ett identitetsindex kommer alltså att användas för i huvudsak samma syfte inom denna verksamhet som i det ärende som i det enskilda fallet föranleder att en identitetsnyckel skapas. Detsamma gäller vid uppdatering av uppgifterna på det sätt som vi beskrivit i avsnitt 14.3. En sådan tillämpning kan sägas ligga i linje med den grundläggande finalitetsprincipen enligt artikel 5.1 b i dataskyddsförordningen, och är enligt vår mening en omständighet som kan vägas in vid bedömningen av om behandlingen av personuppgifter i verksamheteten med ett identitetsindex är proportionerlig; att uppgifter används för ett helt annat syfte bör enligt vår bedömning normalt sett – i vart fall ur den enskildes synvinkel – betraktas som ett större ingrepp i den personliga integriteten.

17.6 Sammantagen bedömning

Genom den nu aktuella proportionalitetsbedömningen tar vi ställning tas till om det finns ett rimligt förhållande mellan hur stort ingreppet i den enskildes personliga integritet kan anses vara med anledning av verksamheten med ett identitetsindex, och hur starkt det behov är som ska tillgodoses genom ingreppet.

17.6.1 Verksamhet med ett identitetsindex medför vissa inskränkningar i grundläggande rättigheter …

När det gäller allvaret i den inskränkning i de grundläggande rättigheterna som verksamhet med ett identitetsindex medför har vi i avsnitt 17.3 identifierat flera faktorer som kan antas medför ett integritetsintrång.

För det första medför verksamheten med ett identitetsindex att personuppgifter – däribland känsliga sådana i form av biometriska uppgifter – om en stor andel av Sveriges befolkning kan komma att behöva lagras och även behandlas på andra sätt. En utökad behandling av biometriska uppgifter för flera miljoner personer innebär ett integritetsintrång och för med sig särskilda risker. Bland annat finns risk för dataintrång som kan ge obehöriga tillgång till de lagrade uppgifterna, vilket i sin tur medför risk för att uppgifterna används av andra aktörer än de avsedda, på sätt som är oförenliga med dataskyddsförordningen och grundläggande rättigheter. Det går inte heller att mildra effekten av ett sådant intrång genom att till exempel byta lösenord eller användarnamn; en ansiktsbild är unik och potentiellt kopplad till den registrerade hela livet.[32] Det är därför av grundläggande betydelse att de tekniska lösningar som behövs för ett system med ett identitetsindex är tillförlitliga, säkra och robusta och att de risker som är kopplade till informations- och cybersäkerhet hanteras på ett betryggande sätt.

Den enskildes möjlighet att avstå från att registreras i ett identitetsindex, och därigenom värja sig mot det integritetsintrång som verksamheten medför, kommer som vi redogjort för i avsnitt 17.3.6 att vara begränsad.

Ett integritetsintrång mildras emellertid på flera olika sätt, vilket vi redogjort för i avsnitt 17.4. Personkretsen är – även om den kommer att omfatta ett stort antal personer – noga avgränsad utifrån identitetsindexets mål och syfte. Vidare är de uppgifter som bör få behandlas också av begränsat antal och utvalda utifrån verksamhetens syfte; någon överskottsinformation skulle enligt vår mening inte komma att behandlas i verksamheten. Aktuella personuppgifter är – förutom ansiktsbild och biometriska uppgifter som kan tas fram ur den – enligt vår bedömning i avsnitt 17.4.3 inte heller av särskilt känslig karaktär.

[32] Jfr Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow, version 1.1, 23 maj 2024, punkt 69 och A29WP Opinion 3/2012 on developments in biometric technologies, s. 34.

Det är vidare tydligt för den enskilde när och under vilka förutsättningar en identitetsnyckel bör kunna skapas och vilka uppgifter om personen som då kan kopplas till den. Det är också förutsebart när uppgifter i verksamheten med ett identitetsindex behöver kunna uppdateras, rättas och raderas. Slutligen har vi i avsnitt 17.4.5 konstaterat att de personuppgifter som behandlas i verksamhet med ett identitetsindex kommer att användas för i huvudsak samma syfte inom den verksamheten som i det ärende som i det enskilda fallet föranleder att en identitetsnyckel skapas.

Oaktat att ett identitetsindex kan komma att omfatta flera miljoner personer bedömer vi att det integritetsintrång som en registrering innebär är förhållandevis begränsat på individnivå. Detta hänför sig delvis till att det – utifrån våra bedömningar – skulle vara tydligt och förutsebart för den enskilde när och hur en identitetsnyckel skapas. Det är som vi pekat på ovan vidare fråga om behandling av ett fåtal personuppgifter om varje individ, som inte möjliggör att någon skapar en större bild av hans eller hennes personliga förhållanden.

Verksamheten med ett identitetsindex som sådan skulle enligt vår mening inte heller vara av särskilt integritetskänslig natur. Det huvudsakliga syftet med ett identitetsindex är att kunna verifiera identitet, med grund i biometriska uppgifter, för personer som i olika sammanhang kommer i kontakt med olika samhällsaktörer. Det är fråga om situationer där det som utgångspunkt bör saknas anledning för den enskilde att inte vilja medverka till att hans eller hennes identitet kan verifieras på ett säkert sätt. Det är, enligt vår bedömning, främst den som på något sätt vill vilseleda någon om sin identitet som kan antas ha andra än principiella invändningar mot en identitetskontroll, i de situationer då en kontroll mot ett index, enligt våra överväganden, bör vara tillåten.

Det är som vi ser det rimligt att anta att endast en liten andel av de personer som registreras i ett identitetsindex kommer att försöka vilseleda myndigheter eller andra aktörer avseende sin identitet. För att ett index ska kunna fylla avsedd funktion krävs det dock att det omfattar en så stor andel som möjligt av dem som vistas i eller har för avsikt att vistas i Sverige eller av annan anledning kan antas komma i kontakt med svenska myndigheter i ett ärende där det finns ett behov av att kunna verifiera personens identitet. Detta eftersom det inte är möjligt att på förhand veta vilka personer som kan komma att missbruka någon annans identitet eller använda multipla identi-

teter. Det är inte heller möjligt att veta vilka personer som kommer att bli utsatta för att någon annan försöker utnyttja deras identitet.

De faktorer som vi lyft fram i avsnitt 17.4, och vad vi i övrigt anfört ovan, talar enligt vår bedömning sammantaget mot att det integritetsintrång som behandlingen av personuppgifter i verksamheten med ett identitetsindex innebär skulle vara oproportionerligt. Till detta kommer skyddsåtgärder i form av bestämmelser om sekretess, sökbegränsningar och begränsningar för elektronisk åtkomst och tekniska åtgärder för att främja informationssäkerhet och cybersäkerhet som bör övervägas, innan ett system med ett identitetsindex införs. Tanken är vidare att möjligheten att verifiera identitet med hjälp av biometriska uppgifter används endast när det är motiverat. Förekomsten av ett system med ett index skulle emellertid kunna antas ha en förebyggande effekt; redan vetskapen om att olika aktörer har möjlighet att genomföra kontroller av biometriska uppgifter för att verifiera en persons identitet kan verka avskräckande, vilket innebär att antalet faktiska kontroller av biometriska uppgifter som skulle genomföras inte nödvändigtvis behöver bli så stort. Detta begränsar också integritetsintrånget.

17.6.2 … men motiveras av ett starkt allmänt intresse

Vår bedömning

Verksamheten med ett identitetsindex, som gör det möjligt att verifiera identitet genom kontroll mot tidigare lagrade ansiktsbilder och biometriska uppgifter som tagits fram ur dessa, kan anses nödvändig och proportionerlig.

Vid en proportionalitetsbedömning ska, som sagt, styrkan av det behov som ska tillgodoses genom inskränkningen i den personliga integriteten beaktas.

I kapitel 10 har vi utvärderat tänkbara åtgärder för stärkt verifiering av identitet och bedömt att ett nytt identitetsindex är ett alternativ som bör utredas för att stärka kopplingen mellan etablerad identitet och verifiering av identitet med grund i biometriska uppgifter. Det övergripande syftet med verksamheten med ett identitetsindex är att motverka sådant identitetsmissbruk som vi redogjort

för i kapitel 9. Detta syfte är som vi ser det av stor betydelse såväl för samhället som för enskilda. Ett system med ett identitetsindex kompletterar de möjligheter att genomföra identitetskontroller med grund i biometriska uppgifter vid etablering av identitet och vid utfärdande av identitetshandlingar som finns idag, eller kommer att finnas vid genomförande av lämnade förslag.

Verksamheten med ett identitetsindex skulle enligt vår bedömning ge dels utökad möjlighet för Polismyndigheten, Migrationsverket och Skatteverket att kontrollera identitet i sådana ärenden där en identitet etableras, dels nya möjligheter för dessa och andra aktörer att verifiera identitet för personer som man möter, med grund i biometriska uppgifter. Att på dessa sätt effektivt motverka att personer som vistas i Sverige uppträder i olika identiteter i olika sammanhang, och att kunna bekräfta att någon är den han eller hon utger sig för att vara, är väsentligt för att kunna motverka identitetsmissbruk. Med hänsyn till de konsekvenser av identitetsmissbruk som vi redogjort för i kapitel 9 bedömer vi att intresset från samhällets sida av att på ett effektivt sätt kunna motverka sådant missbruk väger tungt. Målet med verksamheten med ett identitetsindex är, enligt vår mening, därmed av stor betydelse från samhällssynpunkt. Att intresset av att motverka identitetsbedrägerier och att fastställa identiteten på de personer som vistas i Sverige är ändamål som är godtagbara i ett demokratiskt samhälle, med hänsyn till förebyggande av nationell och allmän säkerhet samt förebyggande av oordning, har lyfts fram i tidigare lagstiftningsärenden. I propositionen *Anpassning av svensk rätt till den reviderade VIS-förordningen* ansåg regeringen exempelvis att detta intresse väger tyngre än det intrång i den personliga integriteten som lagring av de biometriska uppgifter som tas vid en ansökan om nationell visering innebär för den enskilde; intrånget ansågs inte gå utöver målen med lagringen, som bland annat är att underlätta identifiering och undvika identitetsbedrägerier.[33] Den behandling av biometriska uppgifter som utförs med stöd av 15 § utlänningsdatalagen har också i flera lagstiftningsärenden bedömts nödvändig av hänsyn till ett viktigt allmänt intresse, och proportionerlig.[34] Dessa uttalanden har som vi ser det relevans även för bedömningen av verksamheten med ett identitetsindex.

[33] Prop. 2024/25:176, s. 44 f.
[34] Jfr *Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning*, prop. 2017/18:254, s. 35, prop. 2021/22:81, s. 52, *Vissa identitetsfrågor inom utlänningsrätten*, prop. 2020/21:159, s. 22 och prop. 2024/25:176, s. 45.

EU-domstolen har också uttalat sig angående begränsningar av de rättigheter som följer av artikel 7 och 8 i EU:s rättighetsstadga, genom användning av biometriska uppgifter i identifieringssyfte. I mål C-70/18, *Staatssecretaris van Justitie en Veiligheid mot A m.fl.*, konstaterade domstolen att förebyggande av identitetsbedrägerier samt motverkande av olovlig vistelse och inresa utgör ett tvingande skäl av allmänt intresse. Insamling och lagring av biometriska uppgifter i ett nationellt register ansågs göra det möjligt att med säkerhet identifiera en person och upptäcka identitets- och dokumentbedrägerier. Den nationella lagstiftningen var därför ägnad att säkerställa att det eftersträvade syftet uppnåddes. Vidare ansågs lagstiftningen inte gå utöver vad som var absolut nödvändigt för att uppnå målet att förebygga och bekämpa identitets- och dokumentbedrägerier. Vid bedömningen beaktades bland annat behovet av att motverka användning av multipla identiteter, att insamlingen av uppgifterna inte innebär ett ingrepp i intimsfären och inte medför något större fysiskt eller psykiskt obehag för personen och att tillgången till och användningen av personuppgifterna var begränsad. Verksamheten med ett identitetsindex har, enligt vår mening, i fråga om syfte likheter med det register som var för handen i målet.

I förslaget till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem lyftes – i samband med överväganden om proportionalitet – fram bland annat att en korrekt verifiering av identitet för en person kan anses ha en positiv inverkan på rätten till respekt för privatlivet, och i synnerhet rätten till en persons identitet (se artikel 7 i EU:s rättighetsstadga), då detta kan bidra till mindre förvirring kring identiteten.[35] Vid proportionalitetsbedömningen bör därför beaktas att utöver de kontrollmöjligheter som verksamheten med ett identitetsindex ger medför den också ett skydd för enskilda som registreras mot att deras identitet utnyttjas av andra. Rättighetsbegränsningen innebär alltså inte enbart en inskränkning i, utan även ett skydd för, den personliga integriteten och rätten till skydd för personuppgifter (jfr artikel 8 i Europakonventionen och artikel 8 i EU:s rättighetsstadga). Även målet att skydda enskilda är som vi ser det av stor betydelse från samhällssynpunkt.

[35] Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration), COM(2017) 794 final, s. 18.

Vid en sammantagen bedömning anser vi att verksamheten med ett identitetsindex och den inskränkning i den personliga integriteten som den kan medföra, är starkt motiverad av ett allmänt intresse. Vi bedömer därför att verksamheten med ett identitetsindex, som gör det möjligt att verifiera identitet genom kontroll mot tidigare lagrade ansiktsbilder och biometriska uppgifter som tagits fram ur dessa, kan anses vara både nödvändig och utgöra en proportionerlig inskränkning i de rättigheter i fråga om skyddet för den personliga integriteten och privatlivet som följer av bestämmelser i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Verksamheten med ett identitetsindex kan, enligt vår bedömning, också anses proportionerlig på det sätt som avses i artikel 9.2 g i dataskyddsförordningen, vilket innebär att biometriska uppgifter kan behandlas inom ramen för verksamheten. Med detta sagt vill vi understryka att det kan finnas utrymme för att göra en annan bedömning, såväl av lagstiftaren som av bland annat EU-domstolen, vilket vi återkommer till i avsnitt 22.11.

18 Allmänt om användning av ett identitetsindex

18.1 Inledning

I kapitel 11–15 har vi redogjort för våra överväganden kring hur ett identitetsindex skulle kunna etableras, vilka uppgifter det bör innehålla, vilka personer som bör omfattas och hur information i det behöver kunna uppdateras och, under vissa omständigheter, raderas. Det behöver även beskrivas hur ett sådant system skulle kunna användas, på ett sätt som effektivt stärker kopplingen mellan en etablerad identitet och verifiering av denna i olika sammanhang. Användningen av ett identitetsindex bör som utgångspunkt främja att fler aktörer än i dag kan ta del av information om de identiteter som etableras av Polismyndigheten, Migrationsverket och Skatteverket. En viktig utgångspunkt är också att ett index ska kunna främja en användning i många olika ärendeslag och situationer. Om möjligt ska verifiering av identitet också få ske med hjälp av biometriska uppgifter, och vid behov bör ett index kunna användas även för att identifiera en okänd person, vilket är av vikt för att upptäcka användning av multipla identiteter. Dessa mål innebär emellertid att det måste tas i beaktande de risker som behandlingen av personuppgifter och biometriska uppgifter kan medföra, och det integritetsintrång som behandlingen kan medföra för den enskilde. Möjligheten att använda ett index måste med andra ord vara förenlig med dataskyddsförordningen[1], och ska vara proportionerlig. Ett mål om att ett index ska kunna användas av så många aktörer som möjligt, i så många situationer som möjligt, måste alltså vägas mot intrånget i den personliga integriteten. Olika begränsningar kan därför behöva övervägas, exempelvis i fråga om ärendeslag, hur åtkomst till ett sådant system

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

ska fungera och vilken information som en viss aktör bör få tillgång till vid en verifiering eller identifiering mot ett identitetsindex. I detta kapitel behandlar vi ett antal allmänna frågor om användningen av ett index, som till exempel hur en verifiering med hjälp av biometriska uppgifter som utgångspunkt bör gå till och vilka uppgifter som kan lämnas ut, och på vilket sätt. Vissa frågor avseende användningen återkommer vi till i kapitel 21. Med hänsyn till att vi i avsnitt 21.3 bedömer att endast myndigheter bör få använda ett identitetsindex utgår våra överväganden i detta kapitel från det.

18.2 Identifiering

Vårt uppdrag är att främja en stärkt koppling mellan fastställd grundidentitet och *verifiering* av identitet. Ett identitetsindex ska därför kunna användas i vart fall i detta syfte. Eftersom ett sådant system behöver innehålla biometriska uppgifter som har tagits fram ur en ansiktsbild (se avsnitt 11.4.5) kan det även övervägas om det bör vara möjligt att använda ett identitetsindex för att *identifiera* en person, exempelvis om identiteten är okänd. En identifiering mot ett identitetsindex innebär – enligt vår definition av begreppet i avsnitt 7.3.1 – att en sökning görs med hjälp av biometriska uppgifter, för att avgöra om den person som myndigheten möter förekommer med någon identitet, en så kallad en-till-många-jämförelse.

18.2.1 När identifiering bör få användas

Vår bedömning

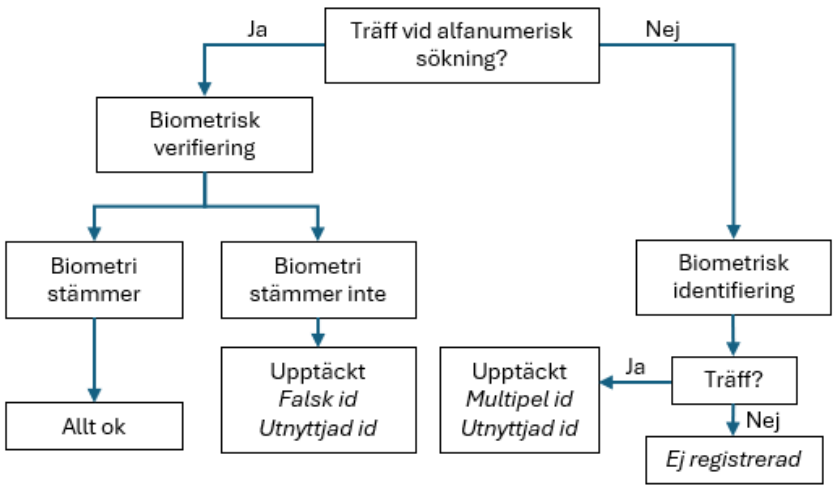
Identifiering av personer i ett identitetsindex bör vara tillåten endast för att Skatteverket, Polismyndigheten och Migrationsverket ska kunna avgöra om en identitetsnyckel ska skapas.

Utifrån vår bedömning i avsnitt 13.2.1 behöver Polismyndigheten, Migrationsverket och Skatteverket – inom ramen för verksamheten med ett identitetsindex – kunna identifiera personer mot ett index, i syfte att säkerställa att endast unika individer registreras och tilldelas en identitetsnyckel. Frågan är om det bör finnas möjlighet att identifiera personer mot ett identitetsindex även i andra situationer

än den nyss nämnda. En sådan möjlighet förutsätter att behandlingen av biometriska uppgifter kan anses stå i proportion till det eftersträvade syftet, nämligen att kunna identifiera en person.

I avsnitt 17.3.1 har vi konstaterat att ett identitetsindex kommer att kunna omfatta ett mycket stort antal personer. Identifiering av en person i ett register som innehåller biometriska uppgifter om ett mycket stort antal personer innebär, av naturliga skäl, ett större integritetsintrång än en biometrisk verifiering mot en specifik individ som har lokaliserats i registret genom en alfanumerisk sökning. En identifiering kräver betydligt mer omfattande behandling av biometriska uppgifter och innefattar – genom att jämförelsen görs en-mot-många – att biometriska uppgifter behandlas för individer som saknar koppling till den situation som föranlett behovet av identifiering. I nedanstående figur åskådliggörs översiktligt behovet av att identifiera personer i andra situationer än vid skapandet av en identitetsnyckel.

Figur 18.1 Behov av identifiering



För att identifiering ska vara möjlig är en grundförutsättning att en ansiktsbild har tagits upp. Det finns därför också normalt en möjlighet att först genomföra en biometrisk verifiering av identitet mot ett identitetsindex med hjälp av ansiktsbilden och de biometriska uppgifter som kan tas fram ur den. Individen måste emellertid först

lokaliseras genom en sökning med en unik alfanumerisk uppgift – en identitetsnyckel, en identitetsbeteckning eller Migrationsverkets individnummer – så att en en-till-en-jämförelse kan göras mot träffen. Om verifieringen misslyckas får myndigheten därigenom en indikation på att personen eventuellt försöker vilseleda myndigheten om vem han eller hon är; med att verifiering misslyckas avser vi att de biometriska uppgifter som är kopplade till den träff som sökningen genererat inte stämmer med de som tagits upp från individen som myndigheten möter. Det kan även vara så att sökningen inte ger någon träff, på grund av det inte finns en identitetsnyckel kopplad till den identitetsbeteckning eller det individnummer som har använts för sökningen och som den enskilde har uppgett.

Oavsett om verifieringen mot ett index misslyckas eller den alfanumeriska sökningen inte ger någon träff kan det vara så att personen är registrerad under någon annan identitet.

I den första situationen kan det enligt vår mening ifrågasättas om det finns ett behov av att kunna identifiera personen mot ett identitetsindex; myndigheten får i detta fall – motsatsvis – anses ha fått svar på den fråga som biometrisk verifiering av identiteten ämnar besvara, nämligen *är personen den som han eller hon utger sig för att vara*? Svaret är i detta fall nej. Detta svar kan mycket väl vara tillräckligt för att myndigheten ska kunna avgöra det ärende som föranledde verifieringen i sak. Som exempel kan nämnas att Pensionsmyndigheten i ett ärende om garantipension skulle kunna neka ansökan från individ A med hänsyn till att han eller hon utger sig för att vara individ B. Pensionsmyndigheten behöver alltså i en sådan situation inte veta vem personen i fråga egentligen är, för att kunna handlägga ärendet om garantipension på ett korrekt sätt. Mot denna bakgrund anser vi att det saknas ett tydligt behov av att identifiera en individ i de fall verifieringen misslyckats på grund av att de biometriska uppgifterna inte stämmer, i vart fall i samband med handläggningen av ett ärende.

Mer problematiskt kan det, som vi ser det, bli när en sökning med den åberopade identiteten inte ger någon träff i ett identitetsindex. En utebliven träff vid en sökning med alfanumeriska uppgifter kan nämligen bero antingen på att en identitetsnyckel helt enkelt saknas för individen i fråga, eller på att en multipel identitet har använts, samtidigt som den enskilde för myndigheten påstår att han eller hon inte är registrerad, som en del i ett försök att vilse-

leda. Om en individ till exempel är registrerad med identitet A hos Migrationsverket och i ett identitetsindex, men med identitet B hos Försäkringskassan, och han eller hon ansöker om en förmån under identitet B, kan detta upptäckas endast om myndigheten kan använda biometriska uppgifter för att identifiera personen genom en sökning mot ett identitetsindex.

Det är som vi ser det inte möjligt för myndigheten att – utan en möjlighet att genomföra en identifiering mot ett index – avgöra om den uteblivna träffen beror på att personen överhuvudtaget inte är registrerad eller om det är fråga om ett vilseledande, och upptäcka en eventuell användning av en multipel identitet. En sökning enbart med alfanumeriska uppgifter skulle inte möjliggöra detta.

En grundförutsättning för att kunna upptäcka en falsk eller multipel identitet genom en identifiering mot ett index är att den person som försöker vilseleda myndigheten har en identitetsnyckel; om person A inte är registrerad i ett identitetsindex och använder sig av identitet B i ovan nämnda kontakt med Försäkringskassan gör en identifieringsmöjlighet det inte möjligt att upptäcka identitetsmissbruket. Det förutsätts vidare att den åberopade identiteten – det vill säga identitet B – *inte* är registrerad – i annat fall kommer identitetsmissbruket att upptäckas redan vid en biometrisk verifiering. Behovet av att kunna identifiera en person mot ett index är alltså, som vi ser det, sammankopplat med hur många personer som är registrerade, även om problemet med att en helt falsk identitet åberopas kan kvarstå över tid. Efter att ett system med ett identitetsindex eventuellt tagits i drift kan det med fog antas att myndigheter och andra aktörer – under en övergångsperiod – i stor utsträckning kommer att möta personer som inte är registrerade. Det kan till exempel antas ta cirka fem år innan majoriteten av svenska medborgare har registrerats, eftersom pass och andra identitetshandlingar som utgångspunkt har en giltighetstid på fem år.[2] Om det ska vara möjligt att identifiera en person på grund av att en sökning med åberopad identitet inte ger någon träff finns det en risk för att ett stort antal identifieringar genomförs ”i onödan” de första åren efter att ett identitetsindex tagits i bruk. Detta innebär också att känsliga personuppgifter behandlas i onödan. Det kan vidare antas att främst personer som inte är registrerade försöker vilseleda myndigheter genom att använda multipla eller falska identiteter; att vara registrerad måste

[2] Jfr kapitel 12 och promemorian *Ett statligt identitetskort*, Ju2026/01595, s. 68.

enligt vår mening rimligtvis ha en viss avskräckande effekt. En identifieringsmöjlighet skulle i de fallen inte vara till nytta.

Med utgångspunkt i våra överväganden i kapitel 13 om när en identitetsnyckel bör kunna skapas – och det uppskattade antalet sådana ärenden per år som vi har redogjort för i avsnitt 17.3.1 – bedömer vi att en klar majoritet av personer som vistas i Sverige skulle kunna vara registrerade i ett identitetsindex inom fem år från att ett sådant system tas i bruk. Det kommer dock att finnas kategorier av personer som inte fångas upp. En sådan kategori utgörs av personer för vilka en identitet etableras i Sverige genom folkbokföring eller genom tilldelning av samordningsnummer, men där Skatteverket av någon anledning inte har tagit upp biometriska underlag i samband med identitetskontrollen (se avsnitt 13.3.6 och 13.3.7). Vi har dock i nämnda avsnitt bedömt att det i den stora majoriteten av sådana ärenden kommer att finnas möjlighet för myndigheten att ta upp biometriska underlag vid en identitetskontroll; när det gäller tredjelandsmedborgare kommer de dessutom med stor sannolikhet att ha registrerats i ett identitetsindex av Migrationsverket vid ett tidigare tillfälle. Även svenska medborgare som folkbokförs i Sverige för första gången eller efter att ha bott utomlands under en tid, kommer förmodligen inte alltid att bli registrerade i ett identitetsindex i samband med folkbokföringen. Det är dock rimligt att anta att dessa kommer att ansöka om ett pass eller en annan identitetshandling och på så sätt registreras i ett index inom en viss tid.

Det kan alltså antas att det kommer att finnas personer som kan vistas och agera i Sverige utan att vara registrerade i ett identitetsindex. Samtliga dessa personer kommer givetvis inte att vara utsatta för att deras identitet utnyttjas. Det bör också beaktas att det utan att identiteten är etablerad i Sverige på något sätt är svårt att till exempel få tillgång till förmåner från välfärdssystemen eller att registreras som ägare till en bil, vilket talar mot att identiteten för personer som inte skulle vara registrerade i ett identitetsindex kan utnyttjas exempelvis för att få tillgång till en välfärdsförmån. De situationer då en etablerad identitet som inte är registrerad i ett index behöver verifieras kan därmed över tid antas bli få. Identiteter som inte är etablerade hos Polismyndigheten, Migrationsverket eller Skatteverket behöver sällan verifieras av andra myndigheter, och när så ändå är fallet behöver de ofta tilldelas ett samordningsnummer för att ärendet ska kunna hanteras av myndigheten; en identitetsnyckel kommer då att

kunna skapas, under förutsättning att Skatteverket tar upp biometriska underlag vid identitetskontrollen.

Ovanstående omständigheter talar enligt vår mening mot att det – i vart fall vid en tidpunkt då ett identitetsindex varit i drift i några år – finns något tydligt behov av att införa en generell möjlighet att identifiera personer när identiteten inte går att verifiera på grund av att den åberopade identiteten inte är registrerad. Det kan även antas att identitetsmissbruk i första hand avser utnyttjande av korrekt etablerade identiteter; i Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* noterades att det är enklare att utnyttja en korrekt utfärdad identitet än att skapa en falsk grundidentitet och att ett allt större problem är att helt korrekta identiteter används av andra personer i olika syften.[3]

Det är alltså i första hand användningen av multipla identiteter som kan antas bestå över tid och som skulle kunna motivera ett behov av identifiering. Att det i Sverige förekommer många individer som är registrerade med multipla identiteter har vi redogjort för i avsnitt 9.2.5. Förekomsten av sådana identiteter kan emellertid antas minska, med hänsyn till de åtgärder som vidtagits och föreslagits i syfte att stärka att en korrekt grundidentitet etableras och de möjligheter att använda biometriska uppgifter som finns, och har föreslagits, för att stärka identitetskontrollen när ett pass eller ett identitetskort utfärdas.

Vi anser visserligen att det kan vara av värde att ge myndigheter en möjlighet att upptäcka användningen av multipla identiteter med hjälp av ett identitetsindex, mot bakgrund av de skador på välfärdssystemen som sådant identitetsmissbruk kan ha, både ekonomiskt och förtroendemässigt. Som vi pekat på ovan finns det dock – i vart fall under en övergångsperiod – en klar risk för att många identifieringar kan komma att göras i ”onödan”. Detta måste enligt vår mening särskilt ses i ljuset av att en identifiering mot ett identitetsindex innebär att ett stort antal biometriska uppgifter behandlas, vilket kan anses innebära ett betydande integritetsintrång. Även om antalet ”onödiga” identifieringar skulle kunna begränsas genom att ett index endast får användas på detta sätt om vissa förutsättningar är uppfyllda – exempelvis om det finns anledning att anta att den person vars identitet ska verifieras biometriskt lämnar oriktiga uppgifter om sin identitet – finns en risk för att detta leder till tillämpningssvårigheter

[3] RiR 2024:12, s. 68.

och osäkerhet om när identifiering får användas. Det skulle i sig kunna leda till att nyttan med en sådan möjlighet går om intet i praktiken.

Särskilt om identifiering i brottsbekämpande verksamhet

Det ovan anförda tar i första hand sikte på behov av att identifiera en person i samband med handläggningen av ett ärende hos en myndighet, exempelvis en ansökan om en förmån av något slag (se avsnitt 21.5.1). En möjlighet att identifiera en person – det vill säga att genom en-till-många-jämförelser mot ett index få svar på frågan *Vem är du?* – skulle kunna vara av betydelse i den brottsbekämpande verksamhet som bedrivs av olika myndigheter. I propositionen *Biometri i brottsbekämpningen* anfördes bland annat det skulle vara mycket värdefullt för möjligheten att klara upp fler brott att tillåta biometriska jämförelser med fingeravtryck och ansiktsbilder även i myndighetsregister som primärt förs för andra än brottsbekämpande ändamål. En sådan reglering skulle väsentligt utöka det jämförelsematerial som polisen kan använda när det finns spår i en brottsutredning i form av fingeravtryck eller ansiktsbilder från en okänd person som misstänks för brott. Det skulle på det sättet bli möjligt att i vissa fall identifiera och lagföra även personer som inte förekommer i polisens biometriregister.[4] Vi delar denna bedömning. Bland annat att föreslogs att biometriska underlag ska få tas upp, registreras och användas vid utredning av brott i större utsträckning samt att vid förundersökning om viss allvarlig brottslighet ska biometriska jämförelser av ansiktsbilder och fingeravtryck av misstänkta gärningsmän få göras mot Migrationsverkets register över fingeravtryck och fotografier. Vidare har förslag lämnats i propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* som innebär att Polismyndigheten ska kunna få göra biometriska jämförelser med ansiktsbilder och fingeravtryck som, vid en sådan reform som föreslås, ska få lagras hos Skatteverket.[5]

Flera olika steg har alltså tagits från lagstiftarens sida för att utöka möjligheterna till biometriska jämförelser i den brottsbekämpande verksamheten mot register som inte förs i sådant syfte. Ett identitets-

[4] Prop. 2024/25:37, s. 131 f.
[5] Prop. 2025/26:261, s. 86 f.

index skulle, även med hänsyn till detta, kunna vara en värdefull jämförelsekälla i den brottsbekämpande verksamheten. Under vårt arbete har Polismyndigheten också lyft fram att myndigheten efterfrågar en möjlighet att kunna använda en-till-många-jämförelser för att kunna identifiera personer som, i olika sammanhang, inte visar upp en giltig identitetshandling.

Vi anser emellertid att det inte är lämpligt att ett identitetsindex används för sådana ändamål, eller för att i brottsbekämpande verksamhet i övrigt identifiera okända personer. I våra direktiv nämns visserligen att det behövs ett perspektivskifte i synen på information för att öka myndigheternas förmåga att förebygga och bekämpa brott. Direktiven innefattar däremot inte ett uppdrag som innebär att vi förväntas lämna förslag som syftar till att stärka den brottsbekämpande verksamheten hos olika myndigheter. Inte heller tar vårt uppdrag sikte på att stärka möjligheten att kunna identifiera okända personer utan på åtgärder som främjar en stärkt koppling mellan en fastställd grundidentitet och *verifiering* av identitet, med grund i biometriska uppgifter, för att säkerställa att en person som en myndighet möter är den som han eller hon utger sig för att vara. Redan detta talar tydligt mot att det i detta sammanhang bör övervägas att låta ett identitetindex användas för identifiering av okända personer i den brottsbekämpande verksamhet som bedrivs av olika myndigheter.

Till detta kommer det integritetsintrång som vi pekat på ovan som uppkommer vid en en-till-många-jämförelse. Sådana faktorer bör enligt vår mening särskilt beaktas i samband med brottsbekämpande verksamhet som, beroende på situationen, kan innehålla betydande inslag av tvång mot den enskilde; det kan i sådana sammanhang vara svårt för både den enskilde och för myndigheten att dra en gräns mellan sådana befogenheter och en utredningsåtgärd i form av identifiering mot ett identitetsindex. Att öppna upp ett index för identifiering inom brottsbekämpande verksamhet skulle under alla omständigheter kräva omfattande överväganden avseende de olika myndigheternas behov och de särskilda dataskyddsrättsliga regelverk som styr denna verksamhet. En mycket noggrann analys av vilka avgränsningar som kan behövas, exempelvis om en identifiering endast bör få användas vid misstanke om ett allvarligt brott, måste också göras.[6]

[6] Jfr de överväganden som gjordes i prop. 2024/25:37, s. 135 ff. och betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 520 ff.

Sammantagen bedömning

Vi anser att det finns ett förhållandevis begränsat behov av att kunna använda ett identitetsindex för identifiering i situationer som har ett samband med handläggning av ett ärende (se avsnitt 21.5.1). Vi gör samma bedömning i fråga om situationer då en myndighet i annat fall, inom ramen för sin verksamhet, genomför en identitetskontroll (se avsnitt 21.5.2). Vidare kan identifiering antas medföra ett betydande integritetsintrång och nyttan får anses avtagande, genom att det efter en viss tid är i relativt få fall som en möjlighet till identifiering kan antas vara effektiv för att upptäcka identitetsmissbruk. Vid en sammanvägd bedömning anser vi att det inte kan anses proportionerligt att ge myndigheter möjlighet att använda ett identitetsindex på detta sätt. Detsamma gäller – utifrån vad vi anfört ovan – för brottsbekämpande verksamhet. Därmed anser vi att identifiering av personer i ett index bör vara tillåten endast för att kunna avgöra om en identitetsnyckel ska skapas.

18.2.2 Uppgifter som behöver göras tillgängliga

Vår bedömning

Om en identifiering inte ger någon träff i ett identitetsindex bör endast en uppgift om det göras tillgänglig. I andra fall bör lagrade uppgifter om identitet, person- och samordningsnummer, Migrationsverkets individnummer och ansiktsbild göras tillgängliga. Vid en markering om skyddade personuppgifter bör även denna uppgift göras tillgänglig.

Frågan är vilka uppgifter som bör kunna göras tillgängliga för Skatteverket, Polismyndigheten och Migrationsverket vid identifiering av en individ mot ett index. För det fall en identifiering – det vill säga en sökning med biometriska uppgifter en-till-många – inte genererar någon träff i ett identitetsindex saknas, enligt vår mening, anledning att lämna ut någon annan uppgift än just detta. Om sökningen däremot ger en eller flera träffar – utifrån hur ett sådant system är konfigurerat i fråga om trösklar för när en matchning ska anses ha skett – behöver den myndighet som genomfört identifieringen däremot

få tillgång till uppgifter om den individ, eller de individer, som sökningen har identifierat.

För det första bör de alfanumeriska uppgifter som är kopplade till individen göras tillgängliga, så att myndigheten kan jämföra dessa med uppgifter om identitet m.m. som den enskilde lämnat. Vi kan inte se att det finns något hinder hänförligt till sekretess mot att från ett identitetsindex göra dessa uppgifter tillgängliga för ovan nämnda myndigheter. Vi kan konstatera att uppgifter i folkbokföringsverksamheten normalt sett anses vara harmlösa och som huvudregel är offentliga.[7] Vi bedömer vidare att det är rimligt att uppgifter i ett identitetsindex om identitet och person- och samordningsnummer, som utgångspunkt, skulle kunna omfattas av sekretess med ett så kallat rakt skaderekvisit. Vi gör samma bedömning när det gäller Migrationsverkets individnummer, det vill säga att en sådan uppgift som huvudregel bör kunna vara offentlig. När dessa uppgifter lämnas ut från ett identitetsindex bör de därför omfattas av motsvarande sekretesskydd hos den myndighet som genomför en identifiering. Vidare kan vi konstatera att uppgifter om personer som är folkbokförda eller har tilldelats ett samordningsnummer är tillgängliga för myndigheter genom Navet, som är Skatteverkets system för distribution av folkbokföringsuppgifter till offentliga aktörer. Utlämnande av uppgift om medborgarskap till allmänheten kan i vissa fall medföra att den enskilde riskerar att lida men. Bestämmelsen i 21 kap. 5 § offentlighets- och sekretesslagen (2009:400) om sekretess med hänsyn till utlännings säkerhet i vissa fall kan dock antas skydda uppgift om medborgarskap även hos den myndighet som genomfört en identifiering mot ett identitetsindex, eftersom bestämmelsen är tillämplig oavsett i vilket sammanhang uppgiften förekommer.

Det är till skillnad från vid en biometrisk verifiering även av vikt att ansiktsbilden kan göras tillgänglig, för att möjliggöra en manuell kontroll även av denna, om detta behövs i det enskilda fallet; i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* gjordes bland annat bedömningen att en automatiserad jämförelse av biometriska underlag kräver även en manuell kontroll av resultatet av jämförelsen. På detta sätt möjliggörs ytterligare ett lager av kontroll för att kunna säkerställa att endast unika individer registreras i

[7] Jfr *Ökat skydd för hotade och förföljda personer samt några åtgärder för att öka kvaliteten i folkbokföringen*, prop. 2017/18:145, s. 29 och *Förslag till sekretesslag m.m.*, prop. 1979/80:2 Del A, s. 210.

ett index. En möjlighet att göra en manuell kontroll är som vi ser det av särskild vikt om identifieringen har genererat flera träffar. Uppgifter i ett identitetsindex om en ansiktsbild skulle enligt vår bedömning rimligtvis behöva omfattas av sekretess med ett så kallat omvänt skaderekvisit, på motsvarande sätt som gäller för ansiktsbilder enligt bestämmelsen i 22 kap. 1 § andra stycket offentlighets- och sekretesslagen angående skydd med hänsyn till enskilds personliga förhållanden i verksamhet med folkbokföring. Det skulle innebära att en ansiktsbild i identitetsindexet endast kan lämnas ut om det står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Vi bedömer att ett sådant skaderekvisit inte skulle utgöra hinder mot att lämna ut en ansiktsbild till Skatteverket, Polismyndigheten och Migrationsverket vid identifiering av en individ mot ett identitetsindex. Detta särskilt som vi i avsnitt 18.5 bedömer att sådana uppgifter omedelbart bör förstöras efter att en identifiering har genomförts.

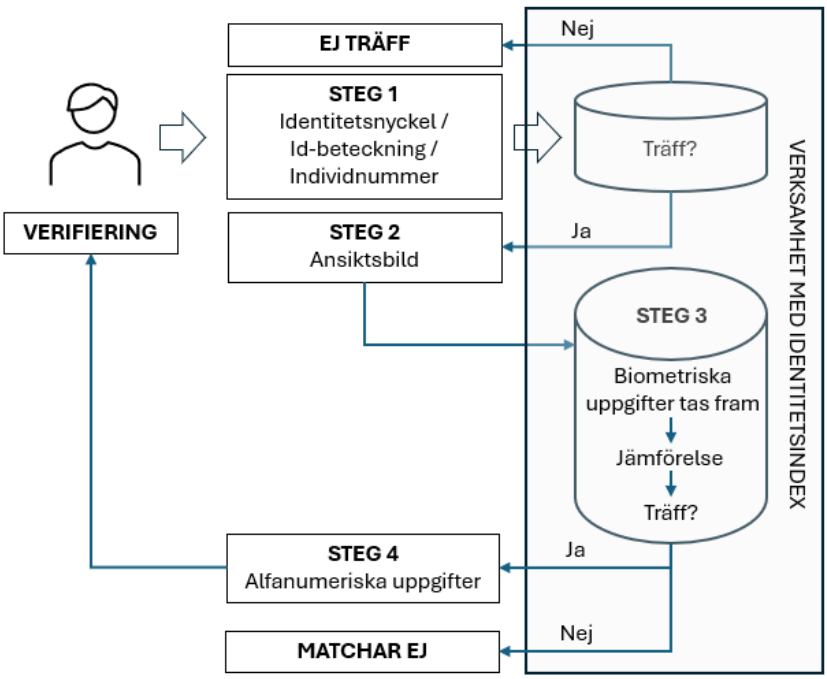
När det gäller de biometriska uppgifter som är kopplade till en viss identitetsnyckel, i form av den biometriska mall som tagits fram från ansiktsbilden för att möjliggöra kontroll av identitet, framstår det inte som nödvändigt att tillgängliggöra dessa uppgifter. En sådan spridning av de biometriska uppgifterna skulle öka riskerna ur ett integritetsskyddsperspektiv och det finns, som vi ser det, inget behov för de aktörer som genomför en identifiering att få tillgång till de biometriska uppgifterna.

I avsnitt 11.4.6, 13.2.2 och 14.3.3 har vi bedömt att en markering om skyddade personuppgifter som finns i folkbokföringsdatabasen avseende namn bör återspeglas i ett identitetsindex, genom att detta markeras i systemet för den aktuella individen. Information om att det finns sådan markering i folkbokföringsverksamheten och som förts över till ett identitetsindex bör, enligt vår bedömning, också kunna lämnas ut vid en identifiering mot indexet. Därmed får den myndighet som får tillgång till uppgifterna vetskap om att uppgifterna är skyddade i folkbokföringen så att myndigheten kan säkerställa en korrekt hantering av uppgifterna med hänsyn till detta.

18.3 Verifiering med hjälp av biometriska uppgifter

Som vi har beskrivit i avsnitt 11.4.5 bör en identitetsnyckel alltid vara kopplad till en ansiktsbild och de biometriska uppgifter som kan tas fram ur denna. För att kunna verifiera en persons identitet genom kontroll mot de biometriska uppgifterna måste rätt individ först lokaliseras i ett index, genom en alfanumerisk sökning. Vid en träff ska en jämförelse av de biometriska uppgifterna som är kopplade till en identitetsnyckel, och den ansiktsbild som tas upp i samband med verifieringen, göras. Detta kan schematiskt beskrivas på följande sätt.

Figur 18.2 Biometrisk verifiering av identitet mot ett identitetsindex



Vi har i avsnitt 7.2.1 redogjort för att vi ser biometrisk verifiering av identitet som en process i två delar. Först behöver en koppling etableras, med hjälp av biometriska uppgifter, till de uppgifter om identitet m.m. som utgör jämförelseunderlag; detta motsvaras av steg 3 i figuren ovan. I ett index behöver en lokalisering dessförinnan

göras med hjälp av alfanumeriska uppgifter (steg 1 i figuren). Därefter görs en jämförelse mellan det jämförelseunderlag som har hämtats – i detta fall från ett identitetsindex – och den påstådda identiteten; i figuren ovan motsvaras detta av steg 4.

18.3.1 Steg 1 – Rätt individ behöver lokaliseras

Vår bedömning

En sökning för att lokalisera en person i ett identitetsindex bör göras i första hand med en identitetsnyckel och i andra hand med person- eller samordningsnummer eller Migrationsverkets individnummer. Sökningen bör inte få göras med identitetsuppgifter.

Det förutsätts att den aktör som vill verifiera identitet biometriskt har tillgång till sådana alfanumeriska uppgifter att personen i fråga kan lokaliseras i ett index. Frågan är om det bör begränsas vilka uppgifter som kan användas i sådant syfte. Detta med hänsyn till att syftet är att lokalisera *en* individ. Det är som vi ser det ur dataskydds- och integritetshänseende inte lämpligt att använda sökbegrepp som innebär att det är sannolikt att flera träffar i systemet genereras, mot vilka jämförelser behöver göras av de biometriska uppgifterna, även om detta skulle vara möjligt. Med utgångspunkt i det identitetsbegrepp som vi definierat i avsnitt 3.2 kan vi konstatera att en sökning med uppgifter om namn, födelsetid eller medborgarskap – eller en kombination av dem – skulle riskera att generera många träffar. Även om sökningen endast resulterar i en träff innebär det inte med säkerhet att träffen avser samma individ som myndigheten möter. Vi anser med hänsyn till detta att en sökning för att lokalisera en individ i ett index, i syfte att genomföra en biometrisk verifiering, inte bör få göras med hjälp av identitetsuppgifter.

För att en biometrisk verifiering mot ett index ska kunna göras förutsätts att personen har en identitetsnyckel; personen kommer av naturliga skäl annars inte att kunna verifieras mot ett identitetsindex. I första hand bör en lokalisering göras genom att denna används. Det är enligt vår mening det lämpligaste sättet eftersom den är garanterat unik. Om individen i det enskilda fallet inte har någon bärare tillgänglig där en identitetsnyckel är lagrad, eller inte kan till-

handahålla en nyckel på något annat sätt, bör i andra hand person- eller samordningsnummer eller Migrationsverkets individnummer användas. Alla som kan komma att vara registrerade i ett index kommer att ha någon av dessa identitets- eller individbeteckningar, och det kan med fog antas att i de situationer som biometrisk verifiering av identitet mot ett identitetsindex kan bli aktuella finns dessa uppgifter också tillgängliga för myndigheten. Som vi redogjort för i avsnitt 11.4.3 och 11.4.4 är uppgifter av nämnda slag unika, och det är därmed i princip uteslutet att mer än en träff genereras. Det kan här lyftas fram att användningen av sådana uppgifter inte förutsätter någon sådan ytterligare medverkan från den enskilde som vid användning av identitetsnyckeln. Detta möjliggör att en sökning skulle kunna göras i fler situationer.

Om sökningen med alfanumeriska uppgifter inte ger någon träff på grund av att en individ med den åberopade identiteten inte är registrerad bör systemet lämna ut endast denna information till den aktör som genomförde sökningen (se avsnitt 18.3.4).

18.3.2 Steg 2 – Upptagning av ansiktsbild

Vår bedömning

Det bör inte regleras i författning hur en ansiktsbild ska tas upp vid verifiering av identitet med hjälp av biometriska uppgifter, exempelvis genom ett krav på personlig inställelse.

När rätt individ som är registrerad i ett index har lokaliserats är det möjligt att verifiera dennes identitet biometriskt genom bland annat en jämförelse av personens ansiktsbild mot de lagrade biometriska uppgifter som tagits fram ur personens ansiktsbild vid ett tidigare tillfälle. Den aktör som vill verifiera en persons identitet på detta sätt kommer alltså att behöva ta upp personens ansiktsbild. Hur detta bör gå till kan variera utifrån omständigheterna i det enskilda fallet. Frågan är om det uttryckligen bör regleras.

Vi kan konstatera att det i flera författningsbestämmelser som ger stöd till myndigheter för att ta upp biometriska underlag inte anges hur detta ska gå till, när det får ske. Ett exempel är 9 kap. utlänningslagen (2005:716). Vissa av ärendeslagen som omfattas

– exempelvis en gränskontroll eller en inre utlänningskontroll – är emellertid till sin natur sådana att den enskilde oftast är närvarande på plats. Även vid en ansökan om uppehållstillstånd är utlänningen normalt närvarande åtminstone vid någon tidpunkt under utredningen av ansökan. Personlig inställelse kan – som vi redogjort för i avsnitt 10.2.3 – i viss mån främja en säkrare identitetskontroll, exempelvis genom att kontroll av fysiska identitetshandlingar kan göras. Det kan då också ställas kontrollfrågor till den enskilde.[8] I ärendeslag som inte naturligen förutsätter personlig närvaro har i vissa fall uttryckligt stöd för att kräva personlig inställelse införts – exempelvis i 26 a § folkbokföringslagen (1991:481) som anger att den som enligt 26 § ska lämna en anmälan om inflyttning från utlandet *ska* inställa sig personligen hos Skatteverket för identitetskontroll, vid vilken biometriska underlag kan tas upp. Kravet på personlig inställelse i nämnda bestämmelse syftar emellertid, som vi ser det, inte primärt till att möjliggöra en upptagning av biometriska underlag utan till att Skatteverket ska kunna göra en tillförlitlig identitetskontroll. Att biometriska underlag kan komma att tas upp i samband med detta är en annan sak.

Upptagning av biometriska underlag av myndigheter förutsätter – med nu tillgängliga och tillämpade tekniska lösningar – att detta görs i samband med personlig inställelse. Vi anser emellertid att det är sannolikt att den tekniska utvecklingen möjliggör att en ansiktsbild tas upp på distans, exempelvis genom att den enskilde själv – med hjälp av en applikation på sin mobiltelefon – tar en bild av sitt ansikte, som kan användas för verifiering av identitet (i avsnitt 27.4 ger vi en teknisk beskrivning av hur detta kan gå till, med befintlig teknik). En ansiktsbild som ska användas som underlag vid en biometrisk verifiering mot ett identitetsindex ska inte heller lagras i indexet eller i något annat register. Det torde därför inte av den anledningen krävas att en ansiktsbild har tagits upp på något särskilt sätt – exempelvis med hjälp av särskild utrustning som bara finns hos en myndighet – eller att den håller samma kvalitet som vid lagring av sådana underlag.

Att alltid kräva personlig inställelse endast i syfte att kunna ta upp biometriska underlag i vad som kan anses utgöra massärenden – exempelvis tillfällig föräldrapenning – skulle i praktiken också kunna medföra en betydande ökad arbetsbörda för myndigheten och opropor-

[8] Jfr *Bolag och brott – några åtgärder mot oseriösa företag*, SOU 2023:34, s. 279 och *Stärkt system för samordningsnummer*, prop. 2021/22:276, s. 36.

tionerliga praktiska svårigheter för enskilda. Vissa av de aktörer som, enligt vår bedömning i kapitel 21 bör få använda biometrisk verifiering mot ett index kanske inte heller har någon praktisk möjlighet att ta upp biometriska underlag vid personlig inställelse. Ett krav på att upptagning ska ske på det sättet skulle därför kunna begränsa användningen i praktiken på ett icke ändamålsenligt sätt.

Vid en sammantagen bedömning av det ovan anförda anser vi att det inte bör regleras i författning hur biometriska underlag i form av ansiktsbild ska tas upp vid verifiering med hjälp av biometriska uppgifter mot ett identitetsindex.

18.3.3 Steg 3 – Jämförelse av biometriska uppgifter

Vår bedömning

Biometriska uppgifter som ska användas för jämförelse med uppgifter som är lagrade i ett identitetsindex bör tas fram ur ansiktsbilden av systemet, inte av den aktör som tar upp ansiktsbilden.

Behandling av personuppgifter i form av biometriska uppgifter är – som vi redogjort för i avsnitt 16.4.2 – enligt artikel 9.1 i dataskyddsförordningen som huvudregel förbjuden. För att behandling av sådana uppgifter alls ska vara tillåten krävs därför att något av undantagen i artikel 9.2 är tillämpligt. Verifiering av identitet med biometriska uppgifter utgör enligt vår bedömning i avsnitt 16.4.1, i verksamheten med ett identitetsindex, behandling av känsliga uppgifter enligt artikel 9.1 i dataskyddsförordningen. I avsnittet har vi bedömt att det i en sådan verksamhet finns stöd för att göra undantag från förbudet i artikel 9.1, med hänvisning till ett viktigt allmänt intresse enligt artikel 9.2 g. Frågan är om användning av ett identitetsindex även kräver att biometriska uppgifter behandlas av den aktör som vill verifiera identitet för en person som aktören möter.

En ansiktsbild utgör inte i sig en biometrisk uppgift enligt definitionen i artikel 4.14 i dataskyddsförordningen. Fotografier som exempelvis bearbetas tekniskt endast för att förbättra bildkvaliteten faller också utanför definitionen.[9] Endast upptagningen av ansiktsbilden utgör enligt vår bedömning inte behandling av en biometrisk upp-

[9] Jfr skäl 51 till dataskyddsförordningen och *Brottsdatalag*, prop. 2017/18:232, s. 85 f. och 435.

gift utan det avgörande är om den som tagit upp bilden bearbetar den på ett sätt som medför att den utgör en biometrisk uppgift. Som vi återkommer till i avsnitt 18.6 bör åtkomsten till ett identitetsindex utformas som en fråga-svar-funktion. Systemet bör alltså lämna ut information efter begäran, inte genom att de aktörer som enligt vår bedömning bör få använda systemet själva kan söka i systemet genom direktåtkomst; det krävs alltså att en myndighet som skulle vara ansvarig för verksamheten med ett identitetsindex, vid varje enskild begäran om verifiering, reagerar på begäran och vidtar de nödvändiga, automatiska, åtgärder som krävs för att behandla begäran. Detta kommer, som vi ser det, att innefatta att vid denna tidpunkt ta fram de biometriska uppgifter ur den inskickade ansiktsbilden som behövs för att en jämförelse ska kunna göras mot lagrade uppgifter. Enligt vår bedömning utförs därför en sådan behandling för att entydigt identifiera en fysisk person som avses i artikel 4.14 först vid denna tidpunkt, inom ramen för verksamheten med ett identitetsindex, genom att särskilda fysiska kännetecken och mätpunkter tas fram ur bilden. Några biometriska uppgifter bör inte heller lämnas ut från verksamheten till den aktör som vill verifiera identitet (se avsnitt 18.3.4).

Den aktör som vill biometriskt verifiera identitet för någon mot ett identitetsindex bör alltså endast skicka in ansiktsbilden i form av biometriska underlag till systemet. Det föreligger, så vitt vi har kunnat utröna, inte några tekniska hinder mot att de biometriska uppgifterna tas fram av systemet vid varje given tidpunkt. Detta med hänsyn till att det endast är fråga om att bearbeta *en* ansiktsbild, inte samtliga bilder som finns lagrade; några sådana tekniska hinder som lyftes fram av Biometriutredningen avseende prestandaförluster vid en identifiering mot ansiktsbilder i vägtrafikregistret gör sig inte gällande (se avsnitt 11.4.5).

Den ovan redovisade ordningen har som vi ser det tydliga fördelar ur integritetssynpunkt, eftersom den innebär att antalet aktörer som behöver behandla biometriska uppgifter begränsas till den eller de myndigheter som skulle vara ansvariga för verksamheten med ett identitetsindex. Med hänsyn till detta anser vi att en aktör som vill verifiera identitet genom jämförelse av ansiktsbild mot biometriska uppgifter i ett index endast bör ta upp och skicka in ansiktsbilden till indexet, utan att själv ta fram biometriska uppgifter ur ansiktsbilden.

18.3.4 Steg 4 – Verifiering av identitet

Vår bedömning

Om en individ inte kan lokaliseras i ett identitetsindex genom en alfanumerisk sökning eller om en biometrisk jämförelse medför en misslyckad matchning bör endast en uppgift om det göras tillgänglig. I andra fall bör lagrade uppgifter om identitet, person- och samordningsnummer och Migrationsverkets individnummer göras tillgängliga. Vid en markering om skyddade personuppgifter bör även denna uppgift göras tillgänglig.

Nästa fråga är vilka uppgifter som ett identitetsindex bör kunna göra tillgängliga för den aktör som vill verifiera identitet med hjälp av biometriska uppgifter.

Om en viss individ inte har kunnat lokaliseras efter en sökning mot ett index med alfanumeriska uppgifter, det vill säga identitetsbeteckning eller Migrationsverkets individnummer, bör endast en uppgift om detta göras tillgänglig. Någon ytterligare information kan i denna situation inte göras tillgänglig, som vi ser det. Den aktör som vill verifiera identitet med hjälp av biometriska uppgifter behöver inte heller någon ytterligare information från systemet. För det fall en identitetsnyckel har använts för att lokalisera individen blir detta av naturliga skäl inte aktuellt. Utifrån informationen att individen inte kunnat lokaliseras med hjälp av den använda sökparametern är det upp till aktören i fråga att ta ställning till om någon annan metod kan användas för att verifiera identitet i det enskilda fallet. De uppgifter som använts för den alfanumeriska sökningen kan också behöva kontrolleras, så att något misstag inte skett vid inmatningen i systemet.

Om en individ som är registrerad i ett identitetsindex har lokaliserats kan den jämförelse som görs mot biometriska uppgifter som är lagrade för honom eller henne resultera i antingen att dessa stämmer överens, eller att de inte matchar. För det fall den biometriska jämförelsen lyckas behöver de alfanumeriska uppgifter som är kopplade till identitetsnyckeln göras tillgängliga, så att aktören kan jämföra dessa med uppgifter om identitet m.m. som den enskilde har lämnat. Stämmer även dessa kan identiteten anses ha verifierats och

aktören har fått svar på frågan om personen är den som han eller hon utger sig för att vara.

På de skäl som anförts i avsnitt 18.2.2 anser vi att det inte finns något hinder hänförligt till sekretess mot att från ett identitetsindex till en myndighet lämna ut uppgifter om identitet, person- och samordningsnummer och Migrationsverkets individnummer för den individ vars identitet har verifierats med hjälp av biometriska uppgifter. När det gäller uppgifter om medborgarskap kan vi konstatera att för personer som är folkbokförda eller som har tilldelats ett samordningsnummer framgår medborgarskap vanligen av folkbokföringen och är i och med det redan tillgängligt för de myndigheter som nyttjar Navet. Eventuell information om att det finns en markering om skyddade personuppgifter i folkbokföringsverksamheten som förts över till ett identitetsindex bör, enligt vår bedömning, också lämnas ut vid en lyckad biometrisk matchning.

Om den biometriska jämförelsen däremot inte lyckats anser vi att endast en uppgift om detta bör lämnas ut. I likhet med ovan anser vi att det i sådana fall saknas anledning att lämna ut ytterligare information. I en sådan situation bör i stället en ny ansiktsbild tas upp, som kan användas för ett nytt verifieringsförsök.

När det gäller ansiktsbilden skulle den visserligen kunna behöva göras tillgänglig för att möjliggöra en manuell kontroll av denna, om detta behövs i det enskilda fallet; i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* gjordes bland annat bedömningen att en automatiserad jämförelse av biometriska underlag kräver även en manuell kontroll av resultatet av jämförelsen.[10] Vi har dock svårt att se att tillgång till en ansiktsbild som finns lagrad i ett index skulle tillföra någon information som innebär att den enskilde aktören på det sättet upptäcker en falsk matchning, i vart fall i fråga om att systemet felaktigt tror sig känna igen en individ; den okulära jämförelsen bör rimligtvis inte kunna ha en högre träffsäkerhet än en datorstödd i detta fall. Vi gör samma bedömning i fråga om de fall då den biometriska jämförelsen inte lyckas. Även om det skulle vara tänkbart att detta beror på att systemet felaktigt tror sig *inte* känna igen den individ vars identitet ska verifieras bedömer vi att en okulär jämförelse inte bör vara den metod som används. Detta är inte heller möjligt om verifieringen sker på distans. Inte heller i övrigt anser vi att det finns skäl att göra en ansiktsbild tillgänglig vid en verifiering med biome-

[10] SOU 2025:75, s. 486.

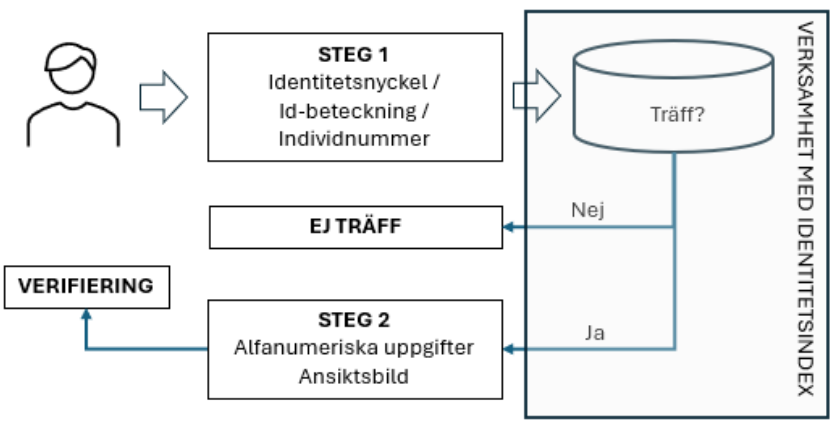
triska uppgifter. Om en biometrisk verifiering inte används är situationen emellertid annorlunda, vilket vi återkommer till i avsnitt 18.4.

När det gäller de biometriska uppgifter som är kopplade till en viss identitetsnyckel, i form av den biometriska mall som tagits fram från en ansiktsbild för att möjliggöra kontroll av identitet, framstår det inte som motiverat att tillgängliggöra dessa uppgifter. En sådan spridning av biometriska uppgifter skulle öka riskerna ur ett integritetsskyddsperspektiv och det finns, som vi ser det, inget behov för en aktör som vill verifiera identitet biometriskt att få tillgång till de biometriska uppgifterna; den nödvändiga jämförelsen görs i systemet. Uppgifterna bör dessutom – enligt vår bedömning i avsnitt 18.5 – förstöras omedelbart efter att kontrollen har genomförts.

18.4 Verifiering med hjälp av en ansiktsbild

Ett sätt att främja en koppling mellan en grundidentitet som har etablerats i ett tidigare ärende och en verifiering av denna skulle kunna vara att ge olika aktörer möjligheter att använda en ansiktsbild som finnas lagrad i ett identitetsindex för en viss individ, för att genom en okulär jämförelse koppla ihop den, och de alfanumeriska uppgifter som är kopplade till den aktuella träffen i indexet, med individen som man möter. Det skulle exempelvis kunna vara av värde när en biometrisk verifiering av något skäl inte kan användas. Verifiering med ansiktsbild kan illustreras på följande sätt.

Figur 18.3 Verifiering med hjälp av ansiktsbild



18.4.1 Steg 1 – Rätt individ behöver lokaliseras

Vår bedömning

När en persons identitet verifieras genom kontroll mot ansiktsbilden i ett identitetsindex bör personen lokaliseras genom en sökning med i första hand en identitetsnyckel och i andra hand person- eller samordningsnummer eller Migrationsverkets individnummer. Sökningen bör inte få göras med identitetsuppgifter.

Med tanke på att ett identitetsindex som utgångspunkt bör få användas av en mycket bred krets aktörer är det ur integritetshänseende av stor vikt att personuppgifter inte behandlas för fler individer än nödvändigt. Till skillnad mot en sådan biometrisk verifiering som vi beskrivit i avsnitt 18.3 förutsätter en verifiering med hjälp av en ansiktsbild att denna görs tillgänglig för den aktör som vill verifiera identitet. Särskilda avvägningar bör därför göras avseende hur den individ vars identitet behöver verifieras med hjälp av en ansiktsbild bör få lokaliseras i ett index.

I avsnitt 18.3.1 har vi bedömt att identitetsuppgifter inte bör få användas för att lokalisera en individ vid en biometrisk verifiering. Vi anser att detsamma bör gälla vid verifiering med hjälp av en ansiktsbild. Detta med hänsyn till att en sökning med sådana uppgifter endast kan ge en upplysning om att det finns *någon* person som är registrerad med den uppgivna identiteten, det vill säga en viss kombination av namn, födelsetid och medborgarskap. Vi har därför svårt att se i vilka situationer som det – i ett möte med en viss individ – skulle vara av värde för myndigheten som vill verifiera identiteten att göra en sökning som utgår från endast identitetsuppgifter. Enligt vår mening är också risken betydande att en sökning med hjälp av identitetsuppgifter genererar flera träffar. Det kan med fog hävdas att det då i praktiken är fråga om en identifiering, dock med alfanumeriska uppgifter; indirekt skulle lokaliseringen behöva göras genom att ansiktsbilder för samtliga träffar manuellt kontrolleras. En sådan behandling av personuppgifter framstår enligt vår mening inte som motiverad ur integritetshänseende. Det bör även erinras om att verifiering av identitet syftar till att besvara frågan *Är personen den som han eller hon utger sig för att vara*; en jämförelse ska alltså göras mot

de uppgifter som är lagrade för honom eller henne, inte mot uppgifter för alla som kan ha vissa identitetsuppgifter.

Vi anser mot denna bakgrund att inte heller vid en verifiering med hjälp av en ansiktsbild bör den individ vars identitet ska verifieras få lokaliseras genom en sökning med identitetsuppgifter. På de skäl som vi anfört i avsnitt 18.3.1 bör i stället personen lokaliseras genom en sökning med i första hand en identitetsnyckel och i andra hand med person- eller samordningsnummer eller Migrationsverkets individnummer.

18.4.2 Steg 2 – Verifiering av identitet

Vår bedömning

Om en individ inte kan lokaliseras i ett identitetsindex bör endast en uppgift om detta göras tillgänglig. I andra fall bör lagrade uppgifter om identitet, person- och samordningsnummer, Migrationsverkets individnummer och ansiktsbild göras tillgängliga. Vid en markering om skyddade personuppgifter bör även denna uppgift göras tillgänglig.

Frågan är vilka uppgifter som behöver tillgängliggöras från ett identitetsindex för att den myndighet som vill verifiera någons identitet med hjälp av en ansiktsbild ska kunna ta ställning till detta. I likhet med vad vi anfört i avsnitt 18.2.2 och 18.3.4 bör det som utgångspunkt sällan vara problematiskt att göra andra uppgifter än ansiktsbilden och de biometriska uppgifterna tillgängliga.

Om en sökning som görs för att lokalisera den individ vars identitet ska verifieras inte ger en träff bör endast en uppgift om *att* individen inte har kunnat lokaliseras göras tillgänglig. Någon ytterligare information bör i denna situation inte göras tillgänglig. Utifrån informationen att individen inte har kunnat lokaliseras med hjälp av den använda sökparametern är det upp till aktören i fråga ta ställning till om någon annan metod kan användas för att verifiera personens identitet i det enskilda fallet.

Verifieringen avser att koppla ihop den individ som en myndighet möter med den identitet som denne gör gällande. En jämförelse behöver då göras mellan å ena sidan de uppgifter som är kopplade till

en viss identitetsnyckel och de som den enskilde har lämnat. För att kunna avgöra vilken identitetsnyckel, och därmed vilka uppgifter, som ska användas måste den kunna kopplas till den individ som myndigheten möter (se avsnitt 7.2.1). Vid en biometrisk verifiering mot ett identitetsindex bekräftas att rätt identitetsnyckel och rätt uppgifter som är kopplade till den har lokaliserats, genom en datorstödd jämförelse av de biometriska uppgifter som är kopplade till identitetsnyckeln och de som tagits fram ur den ansiktsbild som tagits upp i samband med verifieringen. Vid en verifiering med en ansiktsbild måste det i stället göras genom en okulär jämförelse mellan ansiktsbilden som är kopplad till nyckeln och den person som myndigheten möter. Ansiktsbilden är alltså av helt avgörande betydelse för att den som vill verifiera identiteten ska kunna ta ställning till om identiteten kan verifieras. Vi anser därför att ansiktsbilden som är kopplad till en identitetsnyckel som lokaliserats genom en sökning med alfanumeriska uppgifter behöver göras tillgänglig. Vid en verifiering av identitet med hjälp av en ansiktsbild skulle det visserligen vara fråga om göra sådana uppgifter tillgängliga för en större krets av myndigheter. Uppgifterna bör – enligt vår bedömning i avsnitt 18.5 – emellertid omedelbart förstöras efter kontrollen. De alfanumeriska uppgifter som är kopplade till identitetsnyckeln behöver också göras tillgängliga, så att den aktör som ställt begäran kan jämföra dessa med uppgifter om identitet m.m. som den enskilde har lämnat. Utifrån denna jämförelse kan en bedömning göras av om identiteten kan anses verifierad i det enskilda fallet, det vill säga om man har fått svar på frågan om personen är den som han eller hon utger sig för att vara. På de skäl som anförts i avsnitt 18.2.2 anser vi att det inte finns något hinder hänförligt till sekretess mot att lämna ut dessa uppgifter till en myndighet.

De biometriska uppgifter som är kopplade till identitetsnyckeln bör däremot – i likhet med vår bedömning i avsnitt 18.3.4 – inte göras tillgängliga.

18.5 Efterföljande behandling av ansiktsbilder och biometriska uppgifter

Vår bedömning

Den ansiktsbild som tagits upp i syfte att verifiera identitet eller identifiera en person mot ett identitetsindex, och den ansiktsbild som kan ha lämnats ut efter en verifiering eller identifiering, bör omedelbart förstöras efter att kontrollen har genomförts. Detsamma gäller för de biometriska uppgifter som tagits fram ur den ansiktsbild som tagits upp för att möjliggöra kontrollen.

Detta gäller inte när ansiktsbilden och de biometriska uppgifter som tagits fram ur den ska användas för att skapa en identitetsnyckel eller när indexet ska uppdateras med ansiktsbilden och de biometriska uppgifter som tagits fram ur den.

Vid en biometrisk verifiering eller identifiering behöver en ansiktsbild tas upp av den myndighet som vill använda ett identitetsindex i sådana syften. I avsnitt 18.4 har vi bedömt att en ansiktsbild som är lagrad i ett identitetsindex för den individ som lokaliserats genom en alfanumerisk sökning bör kunna göras tillgänglig. Vidare har vi i avsnitt 18.2.2 bedömt att den ansiktsbild som är lagrad i ett index för den individ som lokaliserats genom en biometrisk identifiering bör göras tillgänglig. Frågan är vad som ska hända med de biometriska underlagen efter att kontrollen har genomförts, men även med de biometriska uppgifter som, inom ramen för verksamheten med ett identitetsindex, har tagits fram ur ansiktsbilden vid en biometrisk verifiering eller identifiering.

Någon omständighet som motiverar att en ansiktsbild som tagits upp i syfte att verifiera identitet eller identifiera någon mot ett identitetsindex, eller en ansiktsbild i ett index som kan ha gjorts tillgänglig efter en begäran om verifiering, fortsatt ska få behandlas av den aktör som begärt verifiering av identitet även efter att kontroll av identiteten har genomförts har vi inte funnit. Under alla omständigheter är det inte lämpligt att inom ramen för vårt uppdrag möjliggöra att de aktörer som vi anser bör få verifiera identitet mot ett identitetsindex kan bygga upp egna register med de ansiktsbilder som tagits upp endast i syfte att möjliggöra en verifiering mot ett sådant system. Vi anser därför att såväl den ansiktsbild som tagits upp för att möjliggöra

verifieringen eller identifieringen som den ansiktsbild som en aktör kan ha tagit del av från ett index omedelbart bör förstöras efter att kontrollen har genomförts. Även de biometriska uppgifter som tagits fram ur en ansiktsbild för att möjliggöra en kontroll mot ett index bör förstöras omedelbart efter att kontrollen har genomförts. Genom dessa skyddsåtgärder begränsas behandlingen av ansiktsbilder och de biometriska uppgifter som har tagits fram ur dem.

En ansiktsbild och de biometriska uppgifter som tagits fram ur den bör dock inte förstöras omedelbart efter att en verifiering eller identifiering mot ett identitetsindex har genomförts när de ska användas för att skapa en identitetsnyckel eller när indexet ska uppdateras med ansiktsbilden och de biometriska uppgifter som tagits fram ur den. I dessa fall behövs såväl ansiktsbilden som de biometriska uppgifter som tagits fram ur den i verksamheten med ett identitetsindex.

18.6 Åtkomst och utlämnande av uppgifter

Att en eller flera myndigheter har elektronisk åtkomst till varandras register, databaser eller informationssamlingar är idag en integrerad del i informationsutbytet mellan myndigheter. Såväl vid verifiering av identitet som identifiering mot ett identitetsindex kommer personuppgifter av olika slag, och i olika omfattning, att behöva göras tillgängliga, det vill säga lämnas ut, till den som har ställt begäran. Dataskyddsförordningen saknar bestämmelser som uttryckligen reglerar formen för ett utlämnande av personuppgifter. Om ett utlämnande i sig är tillåtet är det därför normalt upp till den myndighet som lämnar ut uppgifterna att avgöra på vilket sätt detta ska göras. Den personuppgiftsansvarige ska dock säkerställa en lämplig säkerhetsnivå i förhållande till de risker som ett elektroniskt utlämnande kan medföra (jfr artikel 5.1 f och artikel 32 i dataskyddsförordningen). Formerna eller sätten för det elektroniska informationsutbytet mellan myndigheter kan emellertid se olika ut. Vi kan konstatera att det i huvudsak finns två alternativa åtkomstsätt att välja på: direktåtkomst respektive utlämnande på medium för automatiserad behandling, som även benämns annat elektroniskt utlämnande. I detta avsnitt tar vi ställning till hur åtkomsten till ett system med ett identitetsindex bör kunna utformas och vilken av nämnda former av utlämnande som i så fall bör tillämpas.

18.6.1 Elektroniskt utlämnande bör vara tillåtet

Vår bedömning

Elektroniskt utlämnande av uppgifter från ett identitetsindex bör generellt vara tillåtet.

Dataskyddsförordningen ställer inte upp något generellt förbud mot att lämna ut uppgifter i viss form. Trots det är det vanligt att elektroniskt utlämnande regleras särskilt i en registerförfattning, med hänvisning till att ett elektroniskt utlämnande av uppgifter traditionellt sett har ansetts medföra större risk för otillbörliga integritetsintrång, eftersom det ger en större möjlighet att bearbeta och sprida information jämfört med ett utlämnande som sker i pappersform.[11] När det gäller ett identitetsindex är däremot ett elektroniskt utlämnande, som vi ser det, helt avgörande för dess funktion. Teknikutvecklingen har dessutom inneburit en rad integritetshöjande säkerhetsåtgärder vid elektroniskt utlämnande som på många sätt innebär att ett sådant utlämnande inte kan anses utgöra en högre risk för integritetsintrång än utlämnande i pappersform. Det kan därför ifrågasättas om det är korrekt att utgå från att integritetsrisker alltid är lägre vid analogt utlämnande än vid elektroniskt utlämnande.[12]

Med hänsyn till detta anser vi att elektroniskt utlämnande av personuppgifter från ett identitetsindex generellt bör vara tillåtet. Frågan är om det finns anledning att särskilt reglera eller begränsa formerna för elektroniskt utlämnande av uppgifter från ett identitetsindex, genom att till exempel ange att det endast ska få ske antingen genom direktåtkomst eller genom annat elektroniskt utlämnande.

18.6.2 Allmänt om direktåtkomst respektive annat elektroniskt utlämnande

Redan för drygt 15 år sedan konstaterade regeringen att teknikutvecklingen hade lett till att skillnaden mellan direktåtkomst och annat elektroniskt utlämnande blivit så liten att det ibland kunde vara svårt att dra en gräns mellan de olika formerna för elektronisk informa-

[11] Se exempelvis *En omarbetad domstolsdatalag – Anpassning till EU:s dataskyddsförordning*, Ds 2017:41, s. 214.
[12] *Bättre förutsättningar för att utveckla en kunskapsbaserad socialtjänst*, Ds 2024:13, s. 203.

tionsöverföring.[13] Liknande bedömningar har därefter gjorts i flera andra sammanhang. Annat elektroniskt utlämnande kan utformas som en fråga-svar-tjänst, där bedömningen av om en uppgift ska lämnas ut görs automatiserat efter en förfrågan från de mottagande myndigheterna (jfr Högsta förvaltningsdomstolens avgörande HFD 2015 ref. 61, det så kallade LEFI Online-avgörandet). Både direktåtkomst och annat elektroniskt utlämnande kan alltså utformas på sätt som ger mottagaren en mer eller mindre omedelbar tillgång till information från den utlämnande myndigheten och där eventuella sekretessprövningar är gjorda på förhand.

Med *direktåtkomst* avses vanligtvis att en aktör har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. Den som är personuppgiftsansvarig för registret eller databasen har inte någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av.[14] Vid direktåtkomst fattas beslutet om överföring i varje enskilt fall av mottagaren. Prövningen av om ett utlämnande är förenligt med offentlighets- och sekretesslagen måste därför ske redan när uppgifterna görs tillgängliga genom direktåtkomst, oavsett om någon mottagare vid den tidpunkten tar del av dem.[15] Uppgifterna anses alltså utlämnade när direktåtkomst upprättas och blir allmänna hos mottagaren redan vid denna tidpunkt. En förutsättning för direktåtkomst är därför att åtkomsten endast avser uppgifter för vilka det inte gäller sekretess, det vill säga offentliga uppgifter, eller uppgifter som visserligen omfattas av sekretess men som också omfattas av en sekretessbrytande bestämmelse till förmån för den mottagare som får ha direktåtkomst till de aktuella uppgifterna.[16] För att direktåtkomst ska vara möjlig krävs en rad förberedande åtgärder och ställningstaganden avseende exempelvis sekretess, tekniska lösningar, säkerhet och personuppgiftsansvar, i och med att direktåtkomst medför att gränsen mellan de uppgiftsutbytande aktörerna delvis tas bort och innebär att överskottsinformation kan uppstå.

[13] *Utökat elektroniskt informationsutbyte*, prop. 2007/08:160, s. 58.
[14] Jfr *Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling*, prop. 2004/05:164, s. 83, *Kustbevakningsdatalag*, prop. 2011/12:45, s. 133 och *Integritet och effektivitet i polisens brottsbekämpande verksamhet*, prop. 2009/10:85, s. 168.
[15] Se bland annat *Utlänningsdatalag*, prop. 2015/16:65, s. 89 och *Informationsförsörjning på skolområdet*, SOU 2023:21, s. 271 f.
[16] *Transportstyrelsens olycksdatabas*, prop. 2020/21:124, s. 62.

När det gäller *annat elektroniskt utlämnande* är det förenklat sådan elektronisk informationsöverföring som inte är att betrakta som direktåtkomst. Högsta förvaltningsdomstolen har i HFD 2015 ref. 61 gjort en gränsdragning mellan vad som är direktåtkomst och utlämnande på medium för automatiserad behandling (annat elektroniskt utlämnande). Avgörandet rörde begreppet direktåtkomst enligt socialförsäkringsbalken, men Högsta förvaltningsdomstolen har senare gett avgörandet generell tillämplighet (se HFD 2020 not 16). Vid annat elektroniskt utlämnande är det den utlämnande myndigheten som förfogar över prövningen av om och i så fall vilka uppgifter som ska lämnas ut till mottagaren. Ofta utformas detta som en fråga-svar-tjänst. Med en fråga-svar-tjänst kan mottagaren inte söka på annat än tillåtna frågekategorier, exempelvis bara söka efter en individ och inte efter egenskaper.[17] Avgörande för att en sådan teknisk lösning inte ska betraktas som direktåtkomst är att ett utlämnande förutsätter att den utlämnande myndigheten reagerar på en begäran om att de efterfrågade uppgifterna ska lämnas ut. Detta gäller även om reaktionen i sig är helt automatiserad och någon egentlig möjlighet för myndigheten att avbryta utlämnandet inte finns. Den utlämnande myndigheten ska endast behöva göra en prövning av formell art när en uppgift begärs utlämnad, och ska ha juridisk och faktisk kontroll över dessa prövningar och beslut så att en mottagare inte kan styra eller påverka dem utöver att begära att uppgifter ska lämnas ut.[18]

Även ett utlämnande genom en fråga-svar-tjänst kräver vissa förberedande åtgärder. Eftersom ett sådant utlämnande innebär ett automatiserad förfarande behöver vissa frågor behandlas innan tjänsten kan börja användas. Utlämnande myndighet behöver exempelvis ha hanterat frågor om behörighet, sekretess, förekomsten av sekretessbrytande bestämmelser och dataskyddsrättsliga frågor.

[17] *Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården*, SOU 2021:39, s. 192.
[18] eSam, *Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form*, publicerad den 4 maj 2016, s. 23.

18.6.3 Formerna för utlämnande bör regleras särskilt

Vår bedömning

Åtkomst till uppgifter i ett identitetsindex bör ges genom en fråga-svar-tjänst. Utlämnande av uppgifter från ett index bör alltså ske på medium för automatiserad behandling, det vill säga genom annat elektroniskt utlämnande än direktåtkomst.

Direktåtkomst till ett identitetsindex bör inte kunna medges.

Utlämnande av information genom direktåtkomst har historiskt sett förknippats med särskilda risker för den personliga integriteten. Vid direktåtkomst finns det efter det initiala medgivandet ingen möjlighet för den utlämnande myndigheten att påverka eller hindra utlämnande vid ett söktillfälle, vilket innebär en ökad risk för integritetsintrång och för spridning av känsliga uppgifter, bland annat genom att de uppgifter som direktåtkomsten avser blir allmänna handlingar hos mottagaren. Direktåtkomst innebär typiskt sett att information blir tillgänglig för fler personer hos mottagaren och att den utlämnande myndighetens möjligheter att kontrollera hur uppgifterna används minskar.[19] Ju fler personer som har tillgång till uppgifterna, desto mer påtagliga är integritetsriskerna. Även om en direktåtkomst begränsas till att endast omfatta vissa typer av uppgifter som mottagaren har ett faktiskt behov av innebär direktåtkomst ofrånkomligen att denne får teknisk tillgång till fler uppgifter än det kan finnas skäl för; detta brukar benämnas överskottsinformation. Ett utlämnande på medium för automatiserad behandling medför inte motsvarande problem.[20]

Med hänvisning till ovan nämnda risker finns det i regel bestämmelser som förbjuder eller särskilt anger när direktåtkomst får förekomma i registerförfattningar. Exempelvis anges i 19 § utlänningsdatalagen (2016:27) att direktåtkomst till personuppgifter hos Migrationsverket endast får medges vissa i bestämmelsen uppräknade myndigheter och aktörer. En sådan reglering förutsätter dock att det fortfarande är motiverat utifrån ett integritetsperspektiv att göra en juridisk åtskillnad mellan direktåtkomst och annat elektroniskt utlämnande. På samma sätt som dataskyddsförordningen inte reglerar formen eller tekniken för utlämnanden finns det inte heller någon

[19] Se exempelvis prop. 2015/16:65, s. 89.
[20] Se bland annat *Effektivare samverkan för djur- och folkhälsa*, SOU 2025:69, s. 180 ff.

bestämmelse med innebörden att sådan behandling som kan anses vara särskilt integritetskänslig ska regleras särskilt. När det gäller formen för behandling och val av teknisk lösning framhålls i stället i skäl 15 till dataskyddsförordningen att skyddet för den personliga integriteten ska vara teknikneutralt. Vi kan i detta sammanhang notera att regeringen nyligen, i ett lagstiftningsärende avseende i vilken form uppgifter ska få lämnas ut elektroniskt mellan olika aktörer inom vården, har anfört att det inte längre är en stor skillnad mellan direktåtkomst och en elektronisk fråga-svar-tjänst vad gäller risken för integritetsintrång.[21] I slutbetänkandet *Myndighetsdatalag* anfördes bland annat att en väl avvägd direktåtkomst inte behöver innebära större risker än annan form av elektroniskt utlämnande.[22] I departementspromemorian *Bättre förutsättningar för att utveckla en kunskapsbaserad socialtjänst* gjordes bedömningen att mot bakgrund av den allt mindre skillnad som finns mellan direktåtkomst och annat elektroniskt utlämnande saknades det anledning att reglera direktåtkomst särskilt i den i promemorian föreslagna lagen, och att direktåtkomst i stället bör betraktas som en av flera integritetskänsliga former av elektroniskt utlämnande.[23]

Även med beaktande av dessa uttalanden och det allmänna mål om teknikneutralitet som kommer till uttryck i skälen till dataskyddsförordningen finns det enligt vår mening anledning att noga överväga om det just i fråga om åtkomst till ett identitetsindex finns faktorer som gör att formerna för åtkomst till och utlämnande av information från ett sådant system bör regleras särskilt.

En fråga-svar-tjänst kan användas

Frågan är om utlämnande av uppgifter vid en verifiering av identitet eller identifiering kan göras på medium för automatiserad behandling, i form av en sådan fråga-svar-tjänst som det var fråga om i LEFI Online-avgörandet, som nämnts ovan. Utifrån våra överväganden i kapitel 13–15 bör Polismyndigheten, Migrationsverket och Skatteverket ansvara för att skapa en identitetsnyckel och uppdatera den information som finns om individer som är registrerade i ett identitetsindex. Nämnda myndigheter har därmed kontroll över vilken

[21] *Sammanhållen vård och omsorgsdokumentation*, prop. 2021/22:177, s. 79.
[22] SOU 2015:39, s. 151.
[23] Ds 2024:13, s. 204.

information som finns i ett index. Information kan inte ändras av de aktörer som vi anser bör få använda systemet för att verifiera identitet. Hur en verifiering kan gå till har vi beskrivit i avsnitt 18.3 och 18.4. Sammantaget kommer en lokalisering av en individ som behöver göras att ske inom verksamheten med ett identitetsindex – som ovan nämnda myndigheter skulle ansvara för – och systemet bör enligt våra förslag i nyss nämnda avsnitt lämna vissa svar beroende på utfallet av den sökning som görs i verksamheten. Vi anser därmed att det är tydligt att den eller de myndigheter som är ansvariga för verksamheten med ett identitetsindex reagerar på en begäran och genom en prövning avgör om och vilka uppgifter som lämnas ut.

Vi anser med hänsyn till detta att åtkomst och utlämnade av uppgifter från ett identitetsindex vid verifiering av identitet kan ske på medium för automatiserad behandling, det vill säga genom ett annat elektroniskt utlämnande än genom direktåtkomst.

Direktåtkomst bör inte kunna medges

Nästa fråga är om det ur integritetshänseende finns anledning att begränsa utlämnande av information från ett index till utlämnande på medium för automatiserad behandling eller om även direktåtkomst bör kunna medges.

Vi anser, i synnerhet med hänsyn till att ett identitetsindex på sikt skulle kunna innehålla personuppgifter om en stor del av Sveriges befolkning (se avsnitt 17.3.1), att det generellt sett finns anledning att vara restriktiv med att ge tillgång genom direktåtkomst. Till detta kommer att ett syfte med ett identitetsindex är att en bred krets av aktörer kan ta del av information som finns i det. Ett alternativ som visserligen kan övervägas är att medge direktåtkomst endast för en begränsad krets myndigheter, på det sätt som anges i exempelvis 19 § utlänningsdatalagen. Vi anser dock att detta inte är nödvändigt, med hänsyn till att ett utlämnande av uppgifter i form av en fråga-svar-tjänst i praktiken kommer att fylla samma behov av snabb tillgång till information, och upplevas på samma sätt av användarna av ett identitetsindex vid en verifiering av identitet. Det är enligt vår bedömning inte heller möjligt att inom ramen för detta betänkande göra en närmare behovsanalys som tar sikte på den breda krets av

myndigheter som vi anser bör kunna använda ett index, så att en lämplig avgränsning kan göras.

Ett sätt att skydda den personliga integriteten vid direktåtkomst är att begränsa vilka typer av uppgifter eller för vilka ändamål uppgifter får lämnas ut.[24] När det gäller risk för att mottagarna får del av överskottsinformation bör beaktas att ett identitetsindex enligt våra bedömningar i kapitel 11 endast skulle innehålla ett mycket begränsat antal uppgifter om varje individ, vilket talar mot att direktåtkomst innebär större integritetsrisker än utlämnande via en fråga-svar-tjänst. I motsatt riktning talar att den totala mängden uppgifter som kommer att behandlas i ett index kan komma att vara mycket stor. Det är också för ansiktsbilder fråga om uppgifter av känslig art, även om de inte utgör känsliga personuppgifter i dataskyddsförordningens mening. Även om det inte bör vara möjligt att ta del av biometriska uppgifter kan det samtidigt – om direktåtkomst medges – inte uteslutas att den aktör som får sådan tillgång till ett identitetsindex tar fram biometriska uppgifter ur de ansiktsbilder som systemet innehåller. Direktåtkomst skulle enligt vår mening inte heller möjliggöra att olika svar kan lämnas av systemet, på det sätt vi redogjort för i avsnitt 18.3 och 18.4, beroende på resultatet av sökningen. Kontrollen över vilken information som görs tillgänglig skulle som vi ser det begränsas betydligt om direktåtkomst medges. Som en följd av detta – och särskilt då ett identitetsindex bör kunna användas av en bred krets av myndigheter – ökar som vi ser det risken för spridning av personuppgifter.

I förarbetena till utlänningsdatalagen lyftes bland annat fram att direktåtkomst kan innebära effektivitetsvinster för den mottagande myndigheten, eftersom handläggande tjänstemän inte behöver begära ut de uppgifter som behövs för bedömningen av ett enskilt fall från den utlämnande myndigheten, utan själv kan söka den information som krävs i den utlämnande myndighetens personuppgiftssamling. Direktåtkomst kan också innebära fördelar för den utlämnande myndigheten, eftersom den inte behöver avsätta resurser för att hantera de förfrågningar om utlämnande som kommer in från andra myndigheter.[25] Med hänsyn till att en fråga-svar-tjänst normalt utformas så att åtkomsten sker snabbt och automatiserat, anser vi att

[24] Prop. 2020/21:124, s. 63 f.
[25] Prop. 2015/16:65, s. 90.

dessa argument numera inte har någon direkt bäring, i så mån att det talar för ett behov av direktåtkomst till ett identitetsindex.

Sammantaget anser vi att behovet av att utlämnande av information bör kunna ske även genom direktåtkomst inte kan anses vara särskilt framträdande. Ställt mot de potentiella risker för den personliga integriteten som sådan tillgång kan medföra anser vi att utlämnande inte bör få ske genom direktåtkomst. Att det kan finnas en viss fördel i att inte låsa fast det elektroniska utlämnandet i verksamheteten med ett identitetsindex till en fråga-svar-tjänst leder inte till någon annan bedömning. Mot denna bakgrund anser vi att direktåtkomst till ett identitetsindex inte bör få medges.

19 Handlingar som är lämpliga för biometrisk verifiering av identitet

19.1 Inledning

Kontroll av att en person är den som han eller hon utger sig för att vara görs i idag i många sammanhang genom uppvisande av en fysisk identitetshandling. Genom handlingen möjliggörs en koppling mellan individen och en viss registrerad identitet.

Vi har i avsnitt 7.4.2 redogjort för verifiering av identitet genom kontroll mot biometriska underlag i fysiska identitetshandlingar. Vidare har vi i avsnitt 10.5 bedömt att en utökad möjlighet för myndigheter att kontrollera biometriska underlag som är lagrade i en fysisk identitetshandling, eller att ta fram biometriska uppgifter ur en ansiktsbild som är synlig på en identitetshandling för att göra en sådan kontroll, kan främja en stärkt koppling mellan etablerad identitet och verifiering av identitet.

I Sverige finns flera fysiska och elektroniska identitetshandlingar som regelmässigt godtas för att kontrollera vem en person är. Förutsättningarna för utfärdande skiljer sig mellan de olika handlingarna och de utfärdas av olika statliga och privata aktörer för delvis olika syften. Det förekommer också att identitetshandlingar utfärdade i andra länder åberopas vid identitetskontroller i Sverige. Vidare finns det förslag om nya identitetshandlingar som bereds i Regeringskansliet: ett nytt statligt identitetskort med e-legitimation (promemorian *Ett statligt identitetskort*, Ju2026/01595) och en statlig e-legitimation som ska finnas på en fysisk bärare, till exempel det nationella id-kortet (*En statlig e-legitimation*, prop. 2025/26:250). I det här kapitlet utvärderar vi handlingar som skulle kunna vara lämpliga för biometrisk verifiering av identitet, för att stärka kopplingen till en fastställd grundidentitet, i enlighet med våra direktiv. Vid denna utvärdering

beaktar vi de överväganden vi gjort i kapitel 12 om vilka personkategorier som bör omfattas av ett system för att verifiera identitet biometriskt.

Våra överväganden i det här kapitlet tar sikte på ett mer generellt system för att biometriskt verifiera identitet mot en handling och bedömningarna är *inte* avsedda att påverka eller inskränka befintliga och föreslagna möjligheter till sådana kontroller.

19.2 Utgångspunkter

Utgångspunkten för vårt uppdrag är att ett system som syftar till att stärka kopplingen mellan en identitet som har etablerats av en svensk myndighet och verifiering av identiteten, med hjälp av biometriska uppgifter, bör omfatta en så bred personkrets som möjligt. Detta för att systemet ska få ett ändamålsenligt genomslag och kunna vara tillräckligt effektivt i praktiken. Även om det skulle gå att peka ut någon viss krets av personer som mer problematisk i fråga om identitetsmissbruk i Sverige, är ett av syftena med det system som vi har att överväga att skydda individer mot att deras identitet utnyttjas i olika sammanhang. Den gemensamma nämnaren är därför som vi ser det att det är för personer som – på det sätt vi beskrivit i avsnitt 12.2 – har en anknytning till Sverige som det kan finnas ett behov för svenska myndigheter att kunna verifiera identiteten, med hjälp av biometriska uppgifter. Även de resonemang som vi har fört i avsnitt 12.3 går som vi ser det, som utgångspunkt, att applicera vid biometrisk verifiering mot handlingar. De handlingar som kan vara aktuella att använda för biometrisk verifiering bör därför vara de som kan eller ska utfärdas till personer som ingår i de personkategorier som vi i nämnda avsnitt har ansett att det finns ett behov av att biometriskt verifiera identiteten för i olika sammanhang.

Olika kategorier av personer som vistas i landet kan dock inneha olika typer av handlingar som kan användas i detta syfte. Handlingar kan också ha utfärdats i varierande syften, och kan med hänsyn till deras utfärdandeprocess och utformning i olika grad vara lämpliga att använda för biometrisk verifiering av innehavaren. Handlingar kan vid ett visst givet tillfälle vara skadade, antingen för att innehavaren medvetet förstört dem eller av annan anledning. Det kan också vara så att handlingar av någon annan anledning inte kan användas för veri-

fiering eller att personen i fråga helt saknar en viss typ av handling. Detta talar, som vi ser det, för att en så bred flora av handlingar som möjligt bör kunna användas. Det finns vidare anledning att inte begränsa möjliga typer av handlingar på ett sådant sätt att även handlingar som tillkommer senare utesluts; eventuella bestämmelser bör utformas så att de inte kräver en ändring i lag allteftersom handlingar av olika slag tillkommer, eller befintliga ändras på ett sätt som gör dem lämpliga att använda för biometrisk verifiering. Det senare kan exempelvis göras genom att biometriska underlag tillförs ett digitalt lagringsmedium på en handling som endast innehåller en synlig ansiktsbild (se avsnitt 19.2.1).

Ett behov av flexibilitet och av att effektivt kunna fånga upp en ändamålsenlig krets av handlingar – och därmed personer – måste dock ställas mot ett behov av förutsebarhet och tydlighet från lagstiftarens sida. Detta med hänsyn till att biometrisk verifiering mot handlingar innebär ett – om än förhållandevis begränsat (se avsnitt 21.7) – ingrepp i skyddet för den personliga integriteten. Ett grundläggande krav på tydlighet vid verifiering av identitet mot biometriska uppgifter i en handling kan anses följa av EU-domstolens uttalanden i mål C-61/22, *Landeshauptstadt Wiesbaden* (jfr avsnitt 21.3.2). Som vi återkommer till i avsnitt 21.5 anser vi att samtliga myndigheter bör få använda biometrisk verifiering mot handlingar dels när en sådan verifiering är nödvändig vid handläggningen av ett ärende som omfattas av tillämpningsområdet för förvaltningslagen (2017:900), dels när en sådan verifiering, i annat fall, är nödvändig när myndigheten inom ramen för sin verksamhet genomför identitetskontroller. Det är alltså fråga om en betydlig utökning jämfört med när sådan verifiering av identitet är tillåten idag, och enligt lagda förslag.

Även om integritetsinskränkningen inte kan anses bli större – varken i ett bredare perspektiv eller i det enskilda fallet – genom att flera typer av handlingar potentiellt kan användas för biometrisk verifiering anser vi att en avgränsning bör finnas. Att krav på uppvisande av handlingar som omfattas av vissa EU-gemensamma förordningar förutsätter att detta framgår av lag talar i samma riktning (se avsnitt 21.2). Det är som vi ser det inte helt avgörande att så många typer av handlingar som möjligt potentiellt kan användas, för att systemet ska kunna vara effektivt. De handlingar som vi i följande avsnitt anser bör kunna användas är i stället av sådant slag

att det normalt kan förväntas att en person som har en anknytning till Sverige som innebär att hans eller hennes identitet kan behöva verifieras i olika sammanhang, innehar åtminstone någon av dem. En tydlig avgränsning – särskilt i form av en uppräkning av särskilda typer av handlingar som kan användas – är också av vikt för de myndigheter som eventuellt kommer att genomföra sådana kontroller, för att främja en enkel, rättssäker och enhetlig tillämpning.

Det är enligt vår mening svårt att på förhand göra en lämplig avgränsning som är tillräckligt tydlig, utan att den samtidigt blir alltför snäv, vilket skulle kunna påverka genomslaget och ändamålsenligheten negativt. Vissa övergripande avgränsningar – som tar sikte på samtliga möjliga typer av handlingar – anser vi emellertid är möjliga och lämpliga att göra. I första hand anser vi, som vi återkommer till nedan i avsnitt 19.2.1, att endast handlingar som innehåller ett lagringsmedium med biometriska underlag bör komma i fråga. Lagringsmediet behöver även innehålla identitetsuppgifter, dels för att de tryckta identitetsuppgifterna på en handling är lättare att manipulera än motsvarande uppgifter i ett lagringsmedium, dels för att möjliggöra verifiering på distans när det är tekniskt möjligt (se avsnitt 27.4). En avgränsning i form av att endast handlingar med ett lagringsmedium bör omfattas innebär i sig att någon slags bärare förutsätts; den kan i första hand utgöras av ett chip på ett fysiskt kort av något slag men det kan även tänkas att information om biometriska underlag lagras i ett chip på en mobiltelefon, som kan läsas av en applikation på enheten. När det gäller sistnämnda lösning anfördes emellertid i betänkandet *En säker och tillgänglig statlig e-legitimation* – i fråga om en lämplig bärare för en statlig e-legitimation – att det i dagsläget saknas mobiltelefoner som innehåller certifierade säkra chip, att certifiering av säkra chip i mobiltelefoner troligen enbart kommer att vara aktuellt för vissa nyare telefonmodeller och att det även då finns problem gällande hur certifieringen kan upprätthållas i samband med uppdatering av chipen i mobiltelefonen.[1] Med hänsyn till detta anser vi att endast fysiska handlingar bör övervägas.

I övrigt bör, enligt vår bedömning, handlingar med vissa egenskaper särskilt övervägas. Med utgångspunkt i att vårt uppdrag är att stärka kopplingen till en grundidentitet som etablerats av svenska myndigheter bör i första hand rese- och identitetshandlingar som utfärdats av dessa myndigheter omfattas. De handlingar som avses

[1] SOU 2023:61, s. 128 f.

i detta avseende är hemlandspass (se avsnitt 19.3.1) och ett sådant statligt identitetskort som föreslagits i promemorian *Ett statligt identitetskort* (se avsnitt 19.3.2). Alla personer som vistas i Sverige på ett sådant sätt att en anknytning till landet som kan medföra ett behov av att verifiera identiteten uppstår, har emellertid inte alltid tillgång till sådana handlingar, eller väljer att inte ansöka om dem eftersom de har motsvarande utländska handlingar. För att möjliggöra att även dessa personers identitet kan verifieras biometriskt vid behov bör handlingar som en utlänning förväntas inneha vid en vistelse i Sverige särskilt övervägas. Utöver hemlandspass och identitetskort utfärdat av en medlemsstat är ett uppehållstillståndskort utfärdat av svenska myndigheter en sådan typ av handling (se avsnitt 19.3.3).

Sammantaget anser vi att avgränsningen av lämpliga handlingar bör utgå från att en så ändamålsenlig personkrets som möjligt kan komma att omfattas; de bedömningar vi gjort i kapitel 12 avseende personkrets tjänar då, som vi anfört ovan, som utgångspunkt. Detta kan dock nödvändigtvis inte jämställas med att så många typer handlingar som möjligt behöver kunna användas. Vi anser i stället att en tydlighet och relativt snäv avgränsning bör ges företräde.

19.2.1 Handlingen behöver innehålla ett lagringsmedium

Vår bedömning

Handlingar som endast har en synlig ansiktsbild och saknar ett lagringsmedium med biometriska underlag bör inte användas för biometrisk verifiering av identitet.

Vid kontroll av om biometriska underlag som tas upp av innehavaren av en handling stämmer överens med sådana underlag på handlingen är det som utgångspunkt fråga om jämförelse med underlag i ett lagringsmedium på handlingen. Underlagen lagras på ett säkert, krypterat, sätt i ett särskilt chip och kan därför som utgångspunkt inte manipuleras; i exempelvis artikel 1.2 i EU:s passförordning[2] anges att lagringsmediet i pass och resehandlingar som utfärdas av medlemsstaterna ska ha tillräcklig kapacitet och möjlighet att garantera upp-

[2] Rådets förordning (EG) nr 2252/2004 av den 13 december.

gifternas integritet, autenticitet och sekretess. I betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* påpekades emellertid att inte samtliga identitetshandlingar innehåller lagringsmedium med biometriska underlag och att det är enkelt att förstöra ett lagringsmedium på en identitetshandling eller ett uppehållstillståndskort. Vidare uttalades att lagringsmedium inte kunnat läsas vid åtskilliga av de identitetskontroller som Skatteverket gjort i folkbokföringsverksamheten. Med hänsyn till det gjordes bedömningen att Skatteverket i folkbokföringsverksamheten behöver få möjlighet att ta fram biometriska uppgifter även ur en ansiktsbild som är synlig på vissa handlingar, i syfte att biometriskt verifiera innehavarens identitet.[3] Liknande överväganden gjordes av Utredningen om säker och tillgänglig digital identitet; enligt förslagen bör det vid en identitetskontroll i samband med ansökan om den statliga e-legitimation som föreslogs vara tillåtet att göra maskinella jämförelser av fotografiet på en uppvisad identitetshandling, om handlingen saknar ett lagringsmedium och enbart är försedd med ett fotografi eller om lagringsmediet är skadat.[4] Som vi återkommer till i avsnitt 20.2.4 anser vi att underlag i form av en synlig ansiktsbild bör kunna användas för det fall en mer generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar införs.

Extrahering av biometriska uppgifter från en synlig ansiktsbild bör dock ses som en reservmetod, som bara bör tillämpas när det av något skäl inte går att använda ett lagringsmedium på handlingen. Detta med hänsyn till att ansiktsbilden kan manipuleras på ett annat sätt än de biometriska underlag som är lagrade i ett chip. Som vi återkommer till i avsnitt 20.2.4 kan biometrisk verifiering som baseras på biometriska uppgifter som tagits fram ur en synlig ansiktsbild på en handling endast användas vid personlig inställelse, inte på distans. Det är som vi ser det inte möjligt för myndigheten att på distans säkerställa att den bild som används härrör från handlingen och inte någon annan källa. En handling som endast innehåller en synlig ansiktsbild kan också i många fall antas ha utfärdats utan samma nivå av kontroll som när biometriska underlag tas upp i samband med ansökan och lagras på handlingen. En ansiktsbild kan också hålla en lägre kvalitet, som gör att den inte är lämplig att tjäna som underlag

[3] Jfr SOU 2025:75, s. 419 ff. och *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten*, prop. 2025/26:261, s. 103.
[4] SOU 2023:61, s. 168.

för en biometrisk jämförelse. Detta då bilden sannolikt i många fall inte har tagits upp i syfte att kunna användas på detta sätt utan endast för att möjliggöra en enkel, okulär jämförelse. Med hänsyn till att vi i avsnitt 21.3.1 bedömer att biometrisk verifiering mot handlingar bör få användas av en bred krets av myndigheter i många olika ärendeslag, anser vi även att en enhetlig process för verifiering bör eftersträvas.

Att låta myndigheter använda en synlig ansiktsbild på en handling för att ta fram biometriska uppgifter, men samtidigt avgränsa vilka typer av handlingar som bör få användas till sådana som innehåller ett lagringsmedium med biometriska underlag, kan innebära att möjligheteten att använda biometrisk verifiering skulle kunna begränsas på ett icke ändamålsenligt sätt. Vi bedömer emellertid – utifrån våra överväganden i avsnitt 19.3 avseende vilka typer av handlingar som bör användas – att det skulle röra sig om mycket få fall, i första hand personer från tredjeland som har hemlandspass som saknar ett lagringsmedium med biometriska underlag (jfr avsnitt 19.3.1). Dessa personer ska dock, som utgångspunkt, ha ett uppehållstillstånd för att få vistas i Sverige. Det kommer då att vara möjligt att använda ett uppehållstillståndskort för att biometriskt verifiera deras identitet. Vi anser mot denna bakgrund att handlingar som saknar ett lagringsmedium med biometriska underlag inte bör kunna användas för biometrisk verifiering. Sådana handlingar är exempelvis identitetskort som utfärdas av privata aktörer, Skatteverkets id-kort för folkbokförda och SIS-märkta tjänstekort, men även körkort och LMA-kort. Det registreringsbevis för EES-medborgare som föreslogs i betänkandet *Registrering av EES-medborgare*[5] är inte heller aktuellt att använda vid biometrisk verifiering mot handlingar, eftersom det ska vara en enkelt utformad handling utan ett lagringsmedium som innehåller biometriska underlag. Som vi anfört inledningsvis i avsnitt 19.2 behöver lagringsmediet även innehålla identitetsuppgifter; att de inte innehåller *samtliga* uppgifter som ingår i vår definition i avsnitt 3.2 av identitetsbegreppet utgör inte något hinder. De handlingar vi redogör för i avsnitt 19.3.1–19.3.3 har samtliga ett lagringsmedium med både biometriska underlag och identitetsuppgifter (se även avsnitt 27.2 för en teknisk översikt av handlingars innehåll).

[5] SOU 2026:9, s. 164 ff.

19.3 Handlingar som kan vara aktuella att använda

I detta avsnitt belyser vi de typer av handlingar som vi anser framför allt bör kunna användas för biometrisk verifiering, utifrån de kriterier som vi lyft fram i avsnitt 19.2. I fråga om handlingar som utfärdas av svenska myndigheter utgår analysen från såväl befintliga som föreslagna typer av handlingar.

19.3.1 Hemlandspass

Vår bedömning

Hemlandspass som innehåller ett lagringsmedium med biometriska underlag bör kunna användas för att biometriskt verifiera innehavarens identitet.

Pass är en internationellt sett vedertagen identitetshandling som används för verifiering av identitet i mycket stor utsträckning. En mycket stor andel svenska medborgare har ett giltigt pass även om många sannolikt väljer att visa upp andra identitetshandlingar – som till exempel körkort och nationellt identitetskort – inom landet när det behövs.

Svenska hemlandspass regleras i passlagen (1978:302) och i passförordningen (1979:664). Vissa kompletterande bestämmelser finns i Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort (PMFS 2021:3). Pass som utfärdas av medlemsstaterna ska följa de särskilda standarder och krav som framgår av EU:s passförordning[6]. Förordningen innebär harmonisering av säkerhetsdetaljer, inklusive biometriska kännetecken för medlemsstaternas pass och resehandlingar, och det grundläggande målet med förordningen är införande av gemensamma säkerhetsstandarder och interoperabla biometriska kännetecken (skäl 4 och 9). Utformningen ska följa specifikationerna i Internationella civila luftfartsorganisationens (ICAO) dokument om maskinläsbara resehandlingar, dokument 9303 (jfr avsnitt 27.2). Även sådana hemlandspass som utfärdas av tredje

[6] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004.

land innehåller i många fall ett lagringsmedium med biometriska underlag i enlighet med ICAO:s reglering.[7]

Kontroller vid utfärdande av svenska hemlandspass

Ansökan om pass regleras i svensk rätt i 6–6 b §§ passlagen. Sökanden är skyldig att inställa sig personligen och ska styrka sin identitet, sitt svenska medborgarskap och övriga personuppgifter. Polismyndigheten ska noggrant kontrollera den sökandens identitet och sökanden ska i första hand styrka sin identitet genom att visa upp en godtagbar identitetshandling. Om sökanden åberopar handlingar till styrkande av sin identitet eller sitt medborgarskap ska de visas upp i original eller genom vidimerade kopior av original. Polismyndigheten ska granska äktheten hos en uppvisad identitetshandling. Om det uppstår tveksamhet om en uppvisad identitetshandling är giltig eller har utfärdats för sökanden eller för en intygsgivare ska en kontroll göras hos utfärdaren eller tillverkaren av kortet (3 kap. 8 och 9 §§ i PMFS 2021:3). I samband med ansökan är sökanden skyldig att låta Polismyndigheten ta fingeravtryck och en bild i digitalt format av sökandens ansikte (6 §). För barn under sex år och personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck gäller undantag från skyldigheten att låta Polismyndigheten ta upp fingeravtryck (2 § passförordningen). Fingeravtrycken och ansiktsbilden ska sparas i ett lagringsmedium i passet.

En noggrann kontroll av identiteten görs alltså vid ansökan. I promemorian *Ett statligt identitetskort* föreslås vidare en ny pass- och identitetskortsdatalag med tillhörande pass- och identitetskortsdataförordning. Enligt förslagen i promemorian ska ett pass- och identitetskortsregister få innehålla biometriska uppgifter som har tagits fram ur den ansiktsbild som tas av sökanden och när en person ansöker om pass eller statligt identitetskort ska den ansiktsbild som tas av personen få användas för sökning i registret i syfte att kontrollera sökandens identitet och innehav av pass och statligt identitetskort.[8]

[7] *Kontroll av biometriska kännetecken i resehandlingar*, prop. 2017/18:35, s. 10. Enligt ICAO innehåller mer än 140 länders pass biometriska underlag, se ePassport Basics, https://www2023.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx, senast besökt den 15 januari 2026.
[8] Ju2026/01595, s. 139.

Våra överväganden

Hemlandspass innehåller – annat än i vissa undantagsfall – ett lagringsmedium med biometriska underlag och identitetsuppgifter (se avsnitt 27.2), vilket möjliggör en biometrisk verifiering. Sådana kontroller genomförs redan av myndigheter i många olika sammanhang. Som vi redogjort för ovan regleras utfärdande av pass av en EU-gemensam förordning och av internationella standarder, vilket ger en hög tillförlitlighet till utfärdandeprocessen och till de underlag och uppgifter som finns lagrade i en sådan handling; att biometriska underlag tas upp på ett kontrollerat och standardiserat sätt av centrala myndigheter främjar dels korrekta uppgifter, dels kvaliteteten på underlagen. En noggrann identitetskontroll görs också i samband med ansökan. Med hänsyn till inbyggda säkringar av olika slag är en passhandling svår att manipulera. Detta ökar ytterligare möjligheten att använda ett pass för biometrisk verifiering. Vi anser mot denna bakgrund att ett svenskt hemlandspass bör kunna användas för att biometriskt verifiera innehavarens identitet. På detta sätt kan en möjlighet till biometrisk verifiering komma att omfatta en stor del av de personer som har en anknytning till eller är bosatta i Sverige.

När det gäller hemlandspass som utfärdas för medborgare i andra länder har vi ovan konstaterat att vårt uppdrag i första hand är att stärka kopplingen mellan en fastställd grundidentitet och verifiering av identiteten. Det talar för att endast svenska hemlandspass bör omfattas; ett utländskt pass säger till exempel inget i sig om innehavarens koppling till Sverige eller om han eller hon varit i kontakt med svenska myndigheter tidigare och i så fall i vilket sammanhang. Det kan även finnas anledning att i första hand kräva att handlingar som är utfärdade av svenska myndigheter görs tillgängliga för biometrisk verifiering. Det finns enligt vår mening dock ett värde i att även utländska hemlandspass, för vilka det finns särskilda standarder och krav som innebär att handlingen utgör ett säkert verktyg för identifiering, bör kunna användas för en biometrisk verifiering av innehavarens identitet. Som vi nämnt ovan ska hemlandspass i samtliga medlemsstater inom EU utfärdas enligt samma säkerhetsstandarder, och merparten av övriga stater utfärdar hemlandspass som följer internationella standarder, bland annat vad gäller biometri.[9] Att kunna använda även utländska hemlandspass ligger i linje med

[9] Jfr *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 40.

våra direktiv, som anger att målsättningen bör vara att så många som möjligt som vistas i Sverige på sikt ska kunna ingå i ett nytt system för en säkrare verifiering av identitet. Även om tredjelandsmedborgare som vistas mer stadigvarande i landet normalt sett kommer att inneha ett uppehållstillståndskort utfärdat av svenska myndigheter som – enligt vår bedömning i avsnitt 19.3.3 – bör kunna användas för att biometriskt verifiera identitet, finns det kategorier av personer som kan antas använda sitt hemlandspass som främsta identifikationsmedel. Detta gäller till exempel EES-medborgare och familjemedlemmar till dessa, som vistas i landet med uppehållsrätt. Enligt vår bedömning är det av vikt att främja möjligheterna att biometriskt verifiera identiteten även för dessa personer; som vi lyft fram i avsnitt 9.2.4 är ett förekommande upplägg för utnyttjande av identiteter just att EES-medborgare, som utnyttjar sin rätt till fri rörlighet, anmäler inflyttning till Skatteverket i syfte att bli tilldelad ett personnummer som sedan används för olika former av identitetsmissbruk.

Mot denna bakgrund anser vi att även hemlandspass – som innehåller ett lagringsmedium med biometriska underlag – utfärdade av utländska myndigheter bör kunna användas för att biometriskt verifiera innehavarens identitet. Vi återkommer i avsnitt 19.3.4 till främlingspass och resedokument.

19.3.2 Identitetskort

Vår bedömning

Identitetskort som har utfärdats av behörig myndighet och som innehåller ett lagringsmedium med biometriska underlag bör kunna användas för att biometriskt verifiera innehavarens identitet.

Det finns i dagsläget fem svenska fysiska identitetshandlingar som allmänt accepteras som bevis på innehavarens identitet. Dessa är pass, nationellt identitetskort, identitetskort för folkbokförda i Sverige, körkort och SIS-märkt identitetskort. I avsnitt 19.2.1 har vi bedömt att identitetskort för folkbokförda i Sverige och körkort inte bör kunna användas för att biometriskt verifiera innehavarens identitet, då de inte innehåller ett lagringsmedium med biometriska underlag. Detsamma gäller för SIS-märkta identitetskort. I nuläget skulle där-

för – för svensk del – endast nationella identitetskort vara aktuella för att användas för biometrisk verifiering av innehavarens identitet, utöver pass. Vi ska emellertid, enligt våra direktiv, särskilt följa beredningen av förslaget till ett nytt statligt identitetskort som lämnades i betänkandet *Ett säkert statligt ID-kort – med e-legitimation*. I betänkandet föreslogs att de identitetskort som idag betecknas nationellt identitetskort och identitetskort för folkbokförda i Sverige, som utfärdas av Skatteverket, ska ersättas av ett statligt identitetskort med eller utan funktion som resehandling.[10] I promemorian *Ett statligt identitetskort* föreslås också att det nationella identitetskortet ska fasas ut.[11] Vidare har förslag lämnats i *Avveckling av Skatteverkets id-kortsverksamhet* att denna verksamhet ska avvecklas.[12]

Mot denna bakgrund anser vi, i fråga om identitetskort utfärdade av svenska myndigheter, att det är relevant att här närmare belysa om det föreslagna statliga identitetskortet bör kunna användas för att biometriskt verifiera innehavarens identitet.

Kontroller vid utfärdande av ett nytt statligt identitetskort

Det nya statliga identitetskortet ska, enligt förslagen i promemorian *Ett statligt identitetskort*, få utfärdas med eller utan funktion som resehandling till svenska medborgare. Ett identitetskort utan funktion som resehandling ska även få utfärdas till utlänningar som är folkbokförda i Sverige, utlänningar som tilldelats personnummer enligt 18 b § folkbokföringslagen (1991:481) och de som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall samt utlänningar som, efter att ha styrkt sin identitet, har tilldelats ett samordningsnummer enligt lagen (2022:1697) om samordningsnummer och numret inte är förklarat vilande.[13]

Det statliga identitetskortet med resefunktion ska utfärdas med de säkerhetsstandarder, format och specifikationer som anges i EU:s id-kortsförordning.[14] Av artikel 3 i förordningen framgår att de standarder som avses är de som följer av ICAO:s dokument 9303, på samma sätt som för pass (se avsnitt 19.3.1). Det statliga identitets-

[10] SOU 2019:14, s. 216.
[11] Ju2026/01595, s. 171 ff.
[12] Fi2026/01416.
[13] Ju2026/01595j, s. 7.
[14] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.

kortet utan resefunktion omfattas däremot inte av EU:s id-kortsförordning. Det hindrar dock inte att dessa i stora delar får samma utformning och innehåll som de identitetskort som har denna funktion. Det framstår, enligt den ovan nämnda promemorian, tvärtom som lämpligt att förordningens regler om exempelvis storlek, material och tryckmetoder får ligga till grund för utformningen av båda korten.[15] Såvitt vi kan bedöma kommer alltså även det statliga identitetskortet utan resefunktion att utformas i enlighet med vad som följer av EU:s id-kortsförordning – det vill säga ICAO:s dokument 9303 – med undantag för att handlingen inte ska innehålla uppgift om medborgarskap.[16] Vi utgår därför från att både det statliga identitetskortet med och utan resefunktion kommer att innehålla ett lagringsmedium med biometriska underlag och identitetsuppgifter.

Enligt förslagen i promemorian *Ett statligt identitetskort* ska den som ansöker om ett statligt identitetskort vara skyldig att låta den utfärdande myndigheten ta fingeravtryck och en ansiktsbild, som ska lagras på identitetskortet. Skyldigheten att låta myndigheten ta fingeravtryck ska inte gälla för barn under sex år. Fingeravtrycken och de biometriska uppgifter som tas fram ur fingeravtrycken ska dock inte få behandlas i pass- och identitetskortsregistret, men ska få lagras tillfälligt i ärendehanteringssystemet. Ansiktsbilden och de biometriska uppgifter som tas fram ur denna ska dock sparas i registret, men endast få användas som sökbegrepp vid ansökan om pass eller identitetskort för att då kontrollera om sökandens ansiktsbild finns i registret. Vidare föreslogs i promemorian att den utfärdande myndigheten ska få kontrollera om sökandens fingeravtryck och ansiktsbild motsvarar dem som finns på den handling som sökanden använder för att styrka sin identitet. Vid utlämnande av identitetskortet ska myndigheten även få kontrollera om sökandens fingeravtryck och ansiktsbild motsvarar dem som finns lagrade på den handling som ska lämnas ut.[17]

[15] Ju2026/01595, s. 67.
[16] Jfr 2 kap. 1–4 §§ i förslaget till lag om statligt identitetskort i Ju2026/01595, s. 8.
[17] Ju2026/01595, s. 29 och 139.

Våra överväganden

I likhet med hemlandspass som utfärdas av svenska myndigheter eller av en medlemsstat bygger utfärdandet och utformningen av det statliga identitetskort som föreslagits i promemorian *Ett statligt identitetskort* på bestämmelser i en gemensam EU-förordning, nämligen EU:s id-kortsförordning. Detta ger en hög tillförlitlighet till utfärdandeprocessen och till de underlag och uppgifter som finns lagrade i ett identitetskort som utfärdats i enlighet med förordningen; biometriska underlag tas upp på ett kontrollerat och standardiserat sätt av den behöriga myndigheten, vilket främjar dels korrekta uppgifter, dels kvaliteteten på underlagen. Förslag har även lämnats som innebär att vissa kontroller mot andra register och handlingar ska få göras i samband med ansökan. Detta främjar ytterligare att en korrekt handling utfärdas. Med hänsyn bland annat till att det identitetskort för folkbokförda som Skatteverket idag utfärdar föreslås fasas ut kan det antas att det statliga identitetskortet kommer att få ett brett genomslag. Att det föreslås innehålla en statlig e-legitimation talar enligt vår mening i samma riktning och kan antas bidra till att det statliga identitetskortet används i samband med att enskilda legitimerar sig på distans. Sammantaget anser vi därför att det statliga identitetskort – såväl med som utan funktion som resehandling – som föreslagits är lämpligt för att biometriskt verifiera innehavarens identitet. Såväl svenska som utländska medborgares identitet skulle på detta sätt kunna verifieras biometriskt.

Även om det nationella identitetskortet – som vi nämnt ovan – är tänkt att ersättas av det statliga, bör det med hänsyn till sin utformning och till hur det utfärdas också kunna användas för att verifiera identitet biometriskt; av 2–4 §§ förordningen (2005:661) om nationellt identitetskort framgår att sökanden ska inställa sig personligen, att han eller hon ska styrka sin identitet och att biometriska underlag ska tas upp och sparas i ett lagringsmedium i identitetskortet.

När det gäller utländska medborgare – i synnerhet EES-medborgare – är det emellertid inte säkert att de kommer att ansöka om ett svenskt, statligt identitetskort, även med hänsyn till att det föreslås innehålla en svensk e-legitimation, vilket kan vara av praktisk betydelse för den som är bosatt i landet. Det bör därför övervägas om även andra identitetskort bör kunna användas.

Det är som vi ser det inte möjligt att här lämna en detaljerad eller uttömmande uppräkning av vilka existerande och eventuella framtida identitetskort som kan komma i fråga. En grundförutsättning är emellertid, som vi ser det, att det är en handling för vilken det finns särskilda standarder och krav som innebär att den utgör ett säkert verktyg för identifiering. Ett liknande krav framgår exempelvis av Skatteverkets föreskrifter om identitetskontroll vid tilldelning och förnyelse av samordningsnummer, avseende vilka handlingar som får godtas vid en sådan kontroll.[18] Enligt vår bedömning i avsnitt 19.2.1 förutsätts också att handlingen innehåller ett lagringsmedium med biometriska underlag och identitetsuppgifter. Handlingen ska även vara utfärdad av behörig myndighet.

Att de nationella identitetskort som utfärdas av andra medlemsstater i enlighet med EU:s id-kortsförordning uppfyller dessa kriterier är som vi ser det givet. För EES-medborgare som utnyttjar den fria rörligheten och vistas eller bor i Sverige kommer ett statligt identitetskort utan resefunktion att utfärdas av svenska myndigheter endast om personen ansöker om detta och personen är folkbokförd i landet eller har tilldelats ett samordningsnummer efter att ha styrkt sin identitet och numret inte är förklarat vilande. Dessa personer kan alltså ha en fastställd grundidentitet i Sverige – genom folkbokföring eller tilldelning av samordningsnummer – utan att ha ett identitetskort utfärdat av svenska myndigheter. EES-medborgare och medborgare i Schweiz kan – enligt 2 kap. 17 § utlänningsförordningen (2006:97) – även ha rest in i Sverige med ett identitetskort som utfärdats av en behörig myndighet i en EES-stat eller Schweiz. Därmed kan ett identitetskort utfärdat av en annan medlemsstat ligga till grund för etablering av identiteten i Sverige. Det finns därmed indirekt en koppling mellan det utländska identitetskortet och en grundidentitet i Sverige. Det är som vi ser det därför av vikt att även denna kategori av personer kan fångas upp, genom att nationella identitetskort som utfärdats i enlighet med EU:s id-kortsförordning bör kunna användas för en biometrisk verifiering av innehavarens identitet.

Även en tredjelandsmedborgares identitet kan i vissa fall etableras i Sverige trots avsaknad av pass. I dessa fall skulle ett nationellt identitetskort från hemlandet kunna vara av betydelse för att kunna biometriskt verifiera innehavarens identitet. Tredjelandsmedborgare

[18] Se 2 kap. 4 § SKVFS 2023:6.

som saknar pass från hemlandet kommer emellertid normalt sett att ha ett uppehållstillståndskort som kan användas i detta syfte (se avsnitt 19.3.3). För personer som vistas i Sverige med uppehållsrätt som familjemedlem till EES-medborgare förutsätts uppvisande av ett giltigt hemlandspass, enligt artikel 10 i rörlighetsdirektivet[19] (jfr 3 a kap. 9 § utlänningsförordningen). I sådana fall kan hemlandspasset användas för biometrisk verifiering. Det skulle kunna anses tala mot ett behov av att även identitetskort som utfärdats av tredje land bör kunna användas. Att det saknas en gemensam reglering för utfärdande och utformning på det sätt som gäller enligt EU:s id-kortsförordningen talar enligt vår mening också i viss mån för en risk att tillämpningen kan bli otydlig, då ställning behöver tas till om en viss identitetshandling kan anses uppfylla de krav vi lyft fram ovan. Även med hänsyn till detta anser vi att det bör finnas en flexibilitet i vilka identitetskort som kan användas, så länge de uppfyller de grundläggande krav som lyfts fram ovan. En tillräcklig tydlighet och förutsebarhet i fråga om vilka identitetskort som kan användas kan, som vi ser det, i stället uppnås genom att det framgår av föreskrifter som utfärdats av regeringen eller av regeringen utsedd myndighet, i likhet med de föreskrifter som Skatteverket utfärdar i fråga om identitetskontroll, som vi nämnt ovan (se vidare avsnitt 23.9).

Sammantaget anser vi att ett nationellt identitetskort som har utfärdats av behörig myndighet och som innehåller ett lagringsmedium med biometriska underlag bör kunna användas för att biometriskt verifiera innehavarens identitet.

19.3.3 Uppehållstillståndskort

Vår bedömning

Uppehållstillståndskort som utfärdats av svenska myndigheter bör kunna användas för att biometriskt verifiera innehavarens identitet.

Ett stort antal personer vistas i Sverige med uppehållstillstånd av sådan längd att det kan ligga till grund för folkbokföring i landet. Uppgifterna från folkbokföringen kan ligga till grund för andra myn-

[19] Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004.

digheters beslut om bland annat rätt att ta del av olika förmåner. I samband med en sådan prövning kan det finnas ett behov av att biometriskt verifiera identitet. I många fall kan sannolikt ett hemlandspass användas, men det kan finnas personer som saknar en sådan handling. Det kan också vara så att hemlandspasset inte innehåller ett lagringsmedium med biometriska underlag. Frågan är om det bevis om uppehållstillstånd som Migrationsverket *ska* utfärda när uppehållstillstånd beviljas (uppehållstillståndskort) bör kunna användas.

Kontroller vid utfärdande av uppehållstillståndskort

Ett uppehållstillståndskort ska enligt bestämmelsen i 4 kap. 22 § utlänningsförordningen utfärdas i form av en sådan handling som avses i EU-förordningen om uppehållstillståndskort[20]. För uppehållstillstånd som är giltiga i sju dagar eller kortare tid ska något kort emellertid inte utfärdas. Detta framgår av 2 § tredje stycket Migrationsverkets föreskrifter om uppehållstillståndskort, MIGRFS 2022:1. Det saknar betydelse på vilken grund uppehållstillståndet har meddelats. Uppehållstillståndskort utfärdas enligt 4 kap. 19 a § utlänningsförordningen även för personer som beviljas ställning som varaktigt bosatt i Sverige.

Av artikel 4 b i förordningen framgår att de tekniska specifikationerna för insamlingen av biometriska kännetecken ska fastställas i enlighet med förfarandet i artikel 7.2 samt med ICAO:s normer och de tekniska specifikationerna för pass som utfärdas enligt EU:s passförordning. I bilagan till förordningen om uppehållstillståndskort anges att kortet, inklusive biometriska kännetecken, ska utformas som en separat handling, att det ska använda specifikationerna i ICAO:s dokument 9303 och det ska innehålla vissa uppräknade uppgifter, bland annat om innehavarens identitet.

Uppehållstillståndskort utfärdas efter personlig inställelse. Biometriska underlag ska alltid tas upp vid en ansökan om uppehållstillstånd, oavsett grund; av 9 kap. 8 a § utlänningslagen (2005:716) framgår att en utlänning som ansöker om uppehållstillstånd är skyldig att låta Migrationsverket, en utlandsmyndighet eller Regerings-

[20] Rådets förordning (EG) nr 1030/2002 av den 13 juni 2002 om en enhetlig utformning av uppehållstillstånd för medborgare i tredje land.

kansliet fotografera honom eller henne och ta hans eller hennes fingeravtryck. Detsamma gäller om ett uppehållstillståndskort ska utfärdas av en annan anledning än att en utlänning ansöker om uppehållstillstånd. Skyldigheten att låta en myndighet ta fingeravtryck gäller inte om utlänningen är under sex år.

Till skillnad från vid utfärdande av ett svenskt hemlandspass eller ett sådant statligt identitetskort som har föreslagits i promemorian *Ett statligt identitetskort* krävs det inte att utlänningen har styrkt sin identitet för att ett uppehållstillståndskort ska utfärdas. Det kan därför i vissa fall råda osäkerhet om identitetsuppgifterna i handlingen är korrekta, även om en utredning av identiteten görs av Migrationsverket under handläggningen av ett ärende om uppehållstillstånd. Ett uppehållstillståndskort kan till exempel utfärdas till en person som beviljats uppehållstillstånd på grund av behov av internationellt skydd trots att identiteten är oklar. Någon identitetskontroll görs i nuläget inte mot Migrationsverkets eller någon annan myndighets register med hjälp av de biometriska underlag som tas upp med stöd av 9 kap. 8 a § utlänningslagen; enligt nuvarande lydelse av bestämmelsen ska fingeravtryck som inte sparats i ett lagringsmedium på kortet och de biometriska uppgifter som tas fram ur fingeravtrycken och ur fotografiet omedelbarts förstöras när uppehållstillståndskortet har lämnats ut eller ärendet om uppehållstillstånd har avgjorts utan att utlänningen har beviljats uppehållstillstånd. I stället är det de uppgifter som kommit fram i ärendet om uppehållstillstånd – eller om ställning som varaktigt bosatt – som ligger till grund för utfärdandet av kortet. Migrationsverket har emellertid möjlighet att använda biometri för att genomföra sökningar i vissa ärenden om uppehållstillstånd och enligt förslag i regeringens proposition *Stärkt återvändandeverksamhet* ska myndigheten få lagra fingeravtryck och fotografier som tas upp i samband med alla ansökningar om uppehållstillstånd, vilket kan förväntas leda till ökade möjligheter att upptäcka identitetsbedrägerier.[21] Det kan med hänsyn till detta antas att förekomsten av multipla identiteter i Migrationsverkets verksamhet kommer att motverkas framöver och att en person endast kommer att ha ett enda uppehållstillståndskort, i den identitet som är etablerad hos Migrationsverket.

[21] Prop. 2025/26:263, s. 123 f. Förslaget hade ännu inte trätt i kraft vid betänkandets brytpunkt för tryckning.

Våra överväganden

Uppehållstillståndskort innehåller biometriska underlag i ett digitalt och säkert lagringsmedium, vilket möjliggör en biometrisk verifiering. Lagringsmediet innehåller även identitetsuppgifter. Utfärdandet och utformningen av kortet regleras av en EU-gemensam förordning och internationella standarder, vilket ger en hög tillförlitlighet till utfärdandeprocessen och till de underlag och uppgifter som finns lagrade i en sådan handling; att biometriska underlag tas upp på ett kontrollerat och standardiserat sätt av centrala myndigheter främjar dels korrekta uppgifter, dels kvaliteteten på underlagen. Uppehållstillståndskort är enligt vår mening därför till sin utformning lämpliga att använda för biometrisk verifiering av innehavarens identitet. Den omständigheten att identiteten inte behöver vara styrkt förändrar inte bedömningen enligt vår mening; det är i den identitet som framgår av kortet som personen är känd för svenska myndigheter och det är den identiteten som kan ligga till grund för bland annat folkbokföring.

Merparten av de personer som beviljas uppehållstillstånd i Sverige har styrkt sin identitet med ett hemlandspass, mot vilket en biometrisk verifiering bör kunna genomföras (se avsnitt 19.3.1). Vissa personer med uppehållstillstånd i Sverige kan emellertid sakna giltiga identitetshandlingar. De med uppehållstillstånd som folkbokförs i landet eller tilldelas ett samordningsnummer efter att ha styrkt sin identitet kommer visserligen att ha möjlighet att ansöka om ett statligt identitetskort utan resefunktion, vilket kan anses tala mot ett behov av att kontrollera identiteten även mot ett uppehållstillståndskort. Uppehållstillståndskort *ska* däremot utfärdas, vilket innebär att i princip samtliga utlänningar med uppehållstillstånd i Sverige kan förväntas inneha en sådan handling. Personer med kortare uppehållstillstånd som inte kan ligga till grund för folkbokföring och som inte heller har ett samordningsnummer på styrkt identitetsnivå saknar också möjlighet att ansöka om ett statligt identitetskort. För dessa personer kan uppehållstillståndskortet vara den enda handlingen mot vilken en biometrisk verifiering kan göras. Att kunna fånga upp även denna kategori av personer ligger i linje med vårt uppdrag att så många som möjligt som vistas i Sverige på sikt ska kunna ingå i ett nytt system för säkrare verifiering av identitet. Det kommer exempelvis att vara möjligt att på detta sätt biometriskt verifi-

era identitet för vissa personer med samordningsnummer och för personer som beviljats uppehållstillstånd på grunder som inte förutsätter att identiteten har styrkts med ett hemlandspass. Ett uppehållstillståndskort som har utfärdats för en person med uppehållstillstånd i Sverige har – till skillnad mot ett hemlandspass – även den fördelen att det har en direkt koppling till den grundidentitet som etablerats av svenska myndigheter.

Vi kan här konstatera att uppehållstillståndskort används för biometrisk verifiering i andra sammanhang. I 26 b § folkbokföringslagen anges särskilt att den som har beviljats uppehållstillstånd i Sverige på begäran ska överlämna sitt uppehållstillståndskort vid en sådan identitetskontroll som Skatteverket får genomföra enligt 26 a § samma lag. En motsvarande skyldighet finns enligt 2 kap. 3 § lagen om samordningsnummer när en person ska styrka sin identitet i samband med tilldelning av en sådan identitetsbeteckning. Det har alltså i de sammanhangen bedömts lämpligt att kunna genomföra en biometrisk kontroll mot ett uppehållstillståndskort. I regeringens proposition *Åtgärder mot mervärdesskattebedrägerier* föreslogs däremot att endast pass, identitetskort eller annan motsvarande handling ska överlämnas på begäran av Skatteverket vid identitetskontroll i samband med registrering för mervärdesskatt. Uppehållstillståndskort ska alltså inte få kontrolleras i en sådan situation. Anledningen till det utvecklades emellertid inte närmare.[22]

En fråga är om endast uppehållstillståndskort med en viss giltighetstid bör omfattas. Vi har i avsnitt 12.3.3 bedömt att det finns ett behov av att personer som har ett uppehållstillstånd med en giltighetstid som överstiger ett år omfattas av ett identitetsindex, eftersom de kan antas komma att vistas i landet och komma i kontakt med myndigheter i förhållandevis stor utsträckning, vilket innebär att deras identitet behöver verifieras i olika sammanhang. För en person som vistas kortare tid än ett år i Sverige kan behovet av verifiering visserligen generellt sett antas bli mindre än för en person som vistas här under en längre tid. När det gäller ett identitetsindex talar integritetsaspekter mot att lagra uppgifter även för förstnämnda personkategori. Samma skäl gör sig däremot, som vi ser det, inte gällande i fråga om uppehållstillståndskort. I stället bör utgångspunkten här vara att identiteten ska kunna verifieras på bästa möjliga sätt för så

[22] Se *Åtgärder mot mervärdesskattebedrägerier*, prop. 2025/26:128, s. 39 f.

många utlänningar som möjligt som kommer i kontakt med svenska myndigheter, även under en vistelse i Sverige som understiger ett år.

Mot denna bakgrund anser vi att uppehållstillståndskort som är utfärdade av svenska myndigheter bör kunna användas för att biometriskt verifiera innehavarens identitet. Att det inte utgör en identitetshandling utan är ett bevis om att innehavaren har rätt att vistas i Sverige ger som vi ser det – mot bakgrund av den breda personkrets som kan fångas upp och att kortet i andra sammanhang används för biometriska verifiering – inte anledning till en annan bedömning. Vi kan i detta sammanhang konstatera att Migrationsverkets individnummer – som i likhet med ett person- eller samordningsnummer är unikt – varken är tryckt på uppehållstillståndskortet eller lagras i chippet på kortet. Detta ändrar emellertid inte vår bedömning att sådana handlingar är lämpliga att använda för biometrisk verifiering.

När det gäller uppehållstillståndskort som utfärdats av andra EU-medlemsstater – det vill säga för personer som beviljats uppehållstillstånd i en annan medlemsstat än Sverige – anser vi att dessa inte bör omfattas. Visserligen ska dessa kort utfärdas i enlighet med EU-förordningen om uppehållstillståndskort. En sådan handling saknar däremot en koppling till en i Sverige etablerad identitet. Vidare kan en tredjelandsmedborgare med uppehållstillstånd i en annan medlemsstat, som endast har rätt att vistas i Sverige en kortare tid utan uppehållsrätt eller uppehållstillstånd här, enligt vår mening inte antas få en sådan anknytning till landet att det är motiverat att möjliggöra en biometrisk verifiering även med hjälp av det uppehållstillståndskort som utfärdats av en annan medlemsstat. Vi kan även notera att en motsvarande avgränsning framgår av såväl 26 b § andra stycket folkbokföringslagen som 2 kap. 3 § andra stycket lagen om samordningsnummer, som anger att den som beviljats uppehållstillstånd i *Sverige* på begäran ska överlämna sitt uppehållstillståndskort.

19.3.4 Främlingspass och resedokument

Vår bedömning

Främlingspass och resedokument bör inte kunna användas för att biometriskt verifiera innehavarens identitet.

Främlingspass och resedokument utfärdas i Sverige av Migrationsverket och fyller samma funktion, nämligen att utlänningar som inte har och inte heller har möjlighet att skaffa någon handling som gäller som pass ska kunna få en sådan handling. EU:s passförordning omfattar resehandlingar som främlingspass och resedokument; av artikel 1.1 i förordningen framgår att ”pass och *resehandlingar som utfärdas av medlemsstaterna* ska överensstämma med minimisäkerhetsstandarderna i bilagan.” Handlingarna ska därför utformas och utfärdas på samma sätt som gäller för hemlandspass, vilket vi beskrivit i avsnitt 19.3.1, det vill säga utifrån särskilda standarder och krav som innebär att handlingarna utgör ett säkert verktyg för identifiering.[23] Av 11 § Migrationsverkets föreskrifter om främlingspass och resedokument (MIGRFS 2021:11) framgår att bestämmelserna om upptagning, lagring och behandling av biometriska underlag i 6, 6 a och 6 b §§ i passlagen ska tillämpas vid myndighetens handläggning av ärenden om främlingspass och resedokument. Biometriska underlag ska alltså tas upp i samband med ansökan och sparas i ett lagringsmedium i handlingarna.[24]

Våra överväganden

Det krävs inte att utlänningen har styrkt identiteten för att ett främlingspass eller resedokument ska kunna utfärdas av Migrationsverket; av 2 kap. 8 och 13 §§ utlänningsförordningen framgår att handlingarna får förses med en anteckning om att innehavarens identitet inte är styrkt. Vi kan vidare konstatera att varken främlingspass eller resedokument anses utgöra identitetshandlingar, oaktat att de kan användas på väsentligen samma sätt som ett hemlandspass vid internationella resor. Den som har ett främlingspass eller ett resedokument utfärdat av Migrationsverket har sannolikt också ett uppehållstillståndskort. Personer som kommer till Sverige med främlingspass eller resedokument behöver som utgångspunkt uppehållstillstånd för att vistas i landet i mer än 90 dagar per 180-dagarsperiod. Därmed finns det – med utgångspunkt i vår bedömning i avsnitt 19.3.3 – en god möjlighet att använda ett uppehållstillståndskort för att biometriskt verifiera identiteten för samma personkrets som i Sverige kan

[23] Jfr prop. 2021/22:217, s. 68.
[24] *Klarlagd identitet – Om utlänningars rätt att vistas i Sverige, inre utlänningskontroller och missbruk av identitetshandlingar*, SOU 2017:93, s. 131.

få ett främlingspass eller resedokument. Dessa personer kommer – om de är folkbokförda i Sverige eller har ett samordningsnummer på styrkt identitetsnivå – också ha möjlighet att ansöka om ett statligt identitetskort utan resefunktion, under förutsättning att de kan styrka sin identitet. Det kan även antas att de aktuella resehandlingarna utfärdas i samma identitet i vilken uppehållstillstånd har beviljats, vilket i praktiken innebär att det är samma identitetsuppgifter i resehandlingen som i uppehållstillståndskortet.

Sammantaget anser vi att det saknas ett tydligt behov av att kunna använda främlingspass eller resedokument för att biometriskt verifiera innehavarens identitet. Sett tillsammans med att utfärdandet inte kräver styrkt identitet och att de inte utgör en identitetshandling anser vi att främlingspass och resedokument som utfärdats av Migrationsverket eller utländska myndigheter inte bör kunna användas för biometrisk verifiering av innehavarens identitet. Om sådana handlingar har utfärdats av utländska myndigheter saknas även en koppling till en grundidentitet som etablerats av svenska myndigheter.

En avgränsning av detta slag avseende potentiella handlingar som bör kunna användas för biometrisk verifiering kan, som vi ser det, främja en tydlighet och enkelhet i tillämpningen, och tydliggör att fokus ligger på handlingar som har utfärdats i syfte att kunna kontrollera innehavarens identitet, utifrån styrkta uppgifter om denna. Att det i Skatteverkets föreskrifter om identitetskontroll vid folkbokföring samt tilldelning och förnyelse av samordningsnummer[25] – i fråga om vilka typer av handlingar som får godtas vid en sådan kontroll – anges att resedokument och främlingspass utgör en sådan ”annan motsvarande handling” som avses i 26 b § folkbokföringslagen respektive 2 kap. 3 § lagen om samordningsnummer förändrar inte bedömningen. Identitetskontrollerna i dessa sammanhang tar sikte på vissa specifika situationer och klarläggande av identiteten, inte en bredare möjlighet att biometriskt kunna verifiera en grundidentitet som har etablerats i bland annat sådana folkbokföringsärenden. Utformningen av vårt uppdrag medför därför inte att främlingspass och resedokument bör omfattas.

[25] Se 2 kap. 4 § SKVFS 2023:5 och 2 kap. 4 § SKVFS 2023:6.

19.3.5 Uppehållskort samt bevis om uppehållsstatus och bevis för gränsarbetare

Vår bedömning

Uppehållskort samt bevis om uppehållsstatus och bevis för gränsarbetare bör inte kunna användas för att biometriskt verifiera innehavarens identitet.

Migrationsverket ska, enligt 3 a kap. 12 a § utlänningslagen, utfärda ett *uppehållskort* till en EES-medborgares familjemedlem som inte själv är EES-medborgare om han eller hon har ansökt om sådant kort och har uppehållsrätt. Myndigheten ska enligt samma bestämmelse utfärda ett *permanent uppehållskort* till en EES-medborgares familjemedlem som inte själv är EES-medborgare, om han eller hon har ansökt om sådant kort och har permanent uppehållsrätt. När det gäller bevis om upphållsstatus och bevis för gränsarbetare ska dessa utfärdas i form av ett uppehållstillståndskort (3 b kap. 4 och 8 §§ utlänningsförordningen).

Såväl uppehållskort som bevis om uppehållsstatus och bevis för gränsarbetare förutsätter att utlänningen har styrkt sin identitet med hjälp av ett hemlandspass. I samband med ansökan tas biometriska underlag upp, med stöd av 9 kap. 8 g § utlänningslagen, och dessa sparas i ett lagringsmedium i handlingen. Dessa typer av handlingar skulle därför visserligen kunna vara lämpliga för att biometriskt verifiera innehavarens identitet. Vi kan emellertid konstatera att uppehållskort enbart utgör en bekräftelse på den uppehållsrätt som personen redan har och som följer direkt av gemenskapsrätten. Till skillnad från ett uppehållstillståndskort utfärdas dessa handlingar först efter ansökan från den enskilde. Det kan därför inte förväntas att samtliga i den potentiella personkretsen kommer att inneha en sådan handling.

När det gäller personkretsen kan vi konstatera att uppehållskort endast avser tredjelandsmedborgare som är familjemedlem till en EES-medborgare och att bevis om uppehållsstatus och bevis om gränsarbetare endast omfattar brittiska medborgare och deras familjemedlemmar, som vistades i Sverige med uppehållsrätt senast den 31 december 2020. Det är alltså en förhållandevis begränsad krets av personer som omfattas. Ett grundkrav för att uppehållskort ska

utfärdas är dessutom att tredjelandsmedborgaren uppvisar ett giltigt pass, det vill säga ett hemlandspass (jfr 3 a kap. 9 § utlänningsförordningen och Migrationsöverdomstolens avgörande, MIG 2007: 56). En förutsättning för att en tredjelandsmedborgare ska få vistas i Sverige är att han eller hon – enligt 2 kap. 1 § utlänningslagen – har pass. Det finns därmed – med utgångspunkt i vår bedömning i avsnitt 19.3.1 – en god möjlighet att använda hemlandspass för att biometriskt verifiera identitet för samma personkrets som i Sverige kan få ett uppehållskort eller ett bevis om uppehållsstatus och bevis för gränsarbetare.

Mot denna bakgrund ser vi inte något tydligt behov av att kunna använda även nämnda handlingar för att biometriskt verifiera innehavarens identitet. Till detta kommer att ett uppehållskort – och därmed även ett bevis om uppehållsstatus och ett bevis för gränsarbetare – inte är en identitetshandling och inte nödvändigtvis har en koppling till en grundidentitet som har etablerats av den myndighet som utfärdar handlingen. Vid en sammantagen bedömning anser vi därför att varken uppehållskort eller bevis om uppehållsstatus och bevis för gränsarbetare bör kunna användas för att biometriskt verifiera innehavarens identitet.

19.3.6 Elektroniska identitetshandlingar

Vår bedömning

En elektronisk identitetshandling (e-legitimation) innehåller inte i sig biometriska underlag. En sådan handling bör därför, i vart fall inom ramen för ett sådant regelverk som vi överväger, inte kunna användas för att biometriskt verifiera innehavarens identitet.

En elektronisk identitetshandling – som ofta benämns *e-legitimation* – innehåller, liksom en fysisk identitetshandling, uppgifter som entydigt kan kopplas till en viss person. I den reviderade eIDAS-förordningen[26] används begreppet medel för elektronisk identifiering och det var också det begrepp som föreslogs i författningstext i betänkandet *En säker och tillgänglig statlig e-legitimation.*[27] I den efter-

[26] Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024.
[27] SOU 2023:61, s. 125.

följande propositionen *En statlig e-legitimation* används dock begreppet e-legitimation i förslaget till lag om statlig e-legitimation och elektronisk identifiering.[28] I detta betänkande använder vi också begreppet e-legitimation.

Exempel på e-legitimationer i Sverige är BankID och Freja+, som utfärdas av privata aktörer. En e-legitimation kan finnas som en applikation i en mobiltelefon eller en surfplatta eller som en fil på en dator. Den kan också finnas på en fysisk bärare, såsom ett kort. Kortet innehåller då ett chip där informationen lagras. En kortbaserad lösning med ett chip föreslogs av såväl 2017 års ID-kortsutredning i betänkandet *Ett nytt statligt ID-kort – med e-legitimation* som i propositionen *En statlig e-legitimation*. I förstnämnda betänkande föreslogs att det nya statliga identitetskortet – för svenska medborgare och folkbokförda – skulle vara den fysiska bäraren av lagringsmediet[29], medan i delbetänkandet *En säker och tillgänglig statlig e-legitimation* – som ligger till grund för den ovan nämnda propositionen – föreslogs att en statlig e-legitimation ska tillhandahållas på ett kontaktlöst aktivt kort som även är eller kan certifieras som en anordning för att skapa kvalificerade elektroniska underskrifter. Detta kunde enligt utredningen ses som en alternativ lösning för att möta kraven på skyndsamhet att ta fram en statlig e-legitimation. Utredningen bedömde dock att e-legitimation bör finnas även på ett statligt utfärdat identitetskort så snart som möjligt.[30]

I propositionen *En statlig e-legitimation* föreslås att ansiktsbild och eventuella fingertryck ska sparas i ett lagringsmedium *i bäraren* av den statliga e-legitimationen samt att den föreslagna lagen bör innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om e-legitimationens innehåll, bärare och utformning i övrigt, exempelvis vilken fysisk handling som e-legitimationen ska finnas på. För svenska medborgare kan e-legitimationen till exempel placeras på ett identitetskort utfärdat av en passmyndighet, det vill säga för närvarande det nationella identitetskortet. För övriga personkategorier kan föreskrifterna exempelvis avse placering av e-legitimationen på ett kort som i fråga om utformning och innehåll motsvarar ett sådant kort.[31] I promemorian *Ett statligt identitetskort* föreslås att det statliga identitetskortet ska

[28] Prop. 2025/26:250, s. 5 ff.
[29] SOU 2019:14, s. 129.
[30] SOU 2023:61, s. 126 ff.
[31] Prop. 2025/26:250, s. 98.

kunna utfärdas med en e-legitimation och att det ska anges i lag. Med hänsyn till den snabba tekniska utvecklingen bör e-legitimationens utformning och egenskaper i övrigt inte låsas fast i lag. I promemorian anges att e-legitimationen bör finnas i det statliga identitetskortets lagringsmedium, och att e-legitimationen ska innehålla efternamn, förnamn, namns som visas för användaren, personnummer och samordningsnummer.[32] Det kan här förtydligas att den e-legitimation som kommer att utfärdas med stöd av den lag om statlig e-legitimation och elektronisk identifiering som föreslagits i propositionen *En statlig e-legitimation* inte är samma e-legitimation som ska finnas på det statliga identitetskortet. Enligt förslag på övergångsbestämmelser i promemorian *Ett statligt identitetskort* ska bärare av statliga e-legitimationer utfärdade med stöd av lagen om statlig e-legitimation och elektronisk identifiering vara fortsatt giltiga till dess att kortens giltighetstid löper ut. Om den som ansöker om ett statligt identitetskort har en bärare av statliga e-legitimationer utfärdade med stöd av lagen om statlig e-legitimation och elektronisk identifiering ska han eller hon dock vara skyldig att ge in denna för makulering innan det statliga identitetskortet kan lämnas ut.[33] En e-legitimation på det statliga identitetskortet är alltså avsedd att ersätta den e-legitimation som ska utfärdas enligt förslagen i propositionen *En statlig e-legitimation.*

Av artikel 3.2 i eIDAS-förordningen framgår att en e-legitimation är en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster. Förordningen reglerar inte användningen av biometriska underlag eller biometriska uppgifter. I betänkandet *En säker och tillgänglig statlig e-legitimation* gjordes bedömningen att den statliga e-legitimationen även bör kunna användas för att skapa kvalificerade elektroniska underskrifter.[34] En e-legitimation syftar alltså inte i sig till att användas för biometrisk verifiering. Det är som vi ser det viktigt att hålla isär e-legitimationen och bäraren av den; som anfördes i betänkande *Ett nytt statligt ID-kort – med e-legitimation* ska ”den ansiktsbild och de fingeravtryck som lämnas vid ansökan om en statlig e-legitimation, lagras i chipet på bäraren av den statliga e-legitimationen”. I propositionen *En statlig e-legitimation* anfördes att en lagring av innehavarens ansiktsbild och fingeravtryck i den statliga

[32] Ju2026/01595, s. 92 f.
[33] Ju2026/01595, s. 171 f.
[34] SOU 2023:61, s. 139.

e-legitimationen skulle fylla flera viktiga funktioner ur säkerhetssynpunkt; lagringen av uppgifter *i den fysiska bäraren* innebär till exempel att *informationen i bäraren* går att kontrollera med hjälp av biometri. Uppgifterna i den fysiska bäraren skulle till exempel kunna användas av en utfärdande myndighet vid grundidentifieringen i samband med utlämnandet.[35] En e-legitimation innehåller som vi ser det alltså inte i sig några biometriska underlag, men sådana underlag kan däremot sparas i ett lagringsmedium på *bäraren* av e-legitimationen, i syfte att eventuellt kunna genomföra en biometrisk verifiering, för att säkerställa att det är innehavaren av e-legitimationen som använder den. De biometriska underlagen är alltså endast indirekt knutna till en e-legitimation genom att de i ett visst fall har en gemensam bärare.

En e-legitimation utgör visserligen en elektronisk identitetshandling. Som framgår direkt av artikel 3.2 i den reviderade eIDAS-förordningen används sådana handlingar emellertid för *autentisering* för nättjänster. En e-legitimation används alltså, som vi ser det, för att kontrollera behörighet, inte identitet. Vid användningstillfället säger innehavet av e-legitimation inte mer om identiteten hos användaren än exempelvis ett passerkort till en byggnad som har utfärdats till och knutits till en viss person; även om det i samband med utfärdandet kan ha gjorts en noggrann kontroll av identiteten för den som e-legitimationen eller passerkortet utfärdas till, görs ingen säker koppling mellan den personens identitet och den som använder handlingen i samband med användningen, exempelvis vid en ansökan om en förmån som Försäkringskassan handlägger. Att en e-legitimation kan användas för olika former av identitetsmissbruk har vi lyft fram i avsnitt 9.2.4.

Mot denna bakgrund anser vi därför att en e-legitimation i sig inte bör kunna användas för att biometriskt verifiera innehavarens identitet, i vart fall inte med stöd av det regelverk vi överväger. Det krav som följer av artikel 6 i eIDAS-förordningen om att acceptera utländska och anmälda e-legitimationer i nationella digitala tjänster innebär enligt vår bedömning inte ett krav på att en e-legitimation också ska kunna användas för biometrisk verifiering av identitet, enligt nationella bestämmelser i en medlemsstat.

Det ovan sagda utesluter inte att *bäraren* av en e-legitimation kan användas för biometrisk verifiering. Användningen av e-legitimatio-

[35] Prop. 2025/26:250, s. 33.

nen för inloggning i en digital tjänst och en eventuell biometrisk verifiering kommer i dessa fall att kunna utgå från samma fysiska handling, vilket möjliggör en smidig process för innehavaren. I propositionen *En statlig e-legitimation* föreslås vidare att regeringen eller den myndighet som regering bestämmer ska få meddela villkor för användningen av den statliga e-legitimationen. Ett exempel på villkor för ökad säkerhet som nämns är kontroll av biometriska uppgifter i samband med identifiering, eller vid betalningstransaktioner.[36] Det bör dock erinras om att den omständigheten att sådana kontroller kan komma att göras *i samband med* att en e-legitimation används inte innebär att en biometrisk verifiering görs mot e-legitimationen i sig.

Sammanfattningsvis bedömer vi att en elektronisk identitetshandling (e-legitimation), i vart fall inom ramen för ett sådant regelverk vi överväger, inte bör kunna användas för att biometriskt verifiera innehavarens identitet.

19.4 Sammanfattande slutsatser

Vår bedömning

Hemlandspass och identitetskort som utfärdats av behörig myndighet och som innehåller ett lagringsmedium med biometriska underlag bör – inom ramen för ett mer generellt system – kunna användas för att biometriskt verifiera innehavarens identitet. Det bör vara möjligt för regeringen och den eller de myndigheter regeringen bestämmer att närmare specificera mot vilka sådana handlingar en kontroll ska kunna göras.

Även uppehållstillståndskort som utfärdats av svenska myndigheter bör kunna användas för att biometriskt verifiera innehavarens identitet.

Genomgången i detta kapitel visar att det finns flera typer av handlingar mot vilka en biometrisk verifiering, enligt vår bedömning, generellt sett bör kunna göras för att säkrare verifiera en persons identitet. Dessa är – utifrån de bedömningar som vi gjort i avsnitt 19.3 – som utgångspunkt hemlandspass och identitetskort som utfärdats

[36] Prop. 2025/26:250, s. 42 f.

av behörig myndighet och som innehåller ett lagringsmedium med biometriska underlag, samt uppehållstillståndskort som utfärdats av svenska myndigheter. Med utgångspunkt i dessa handlingar bedömer vi att det skulle vara möjligt att biometriskt verifiera identiteten för i princip alla personer med sådan anknytning till Sverige som vi i avsnitt 12.3 bedömt att det finns ett behov för svenska myndigheter att kunna verifiera identiteten biometriskt för. Även personer som beviljats uppehållstillstånd för kortare tid än ett år kommer, utifrån våra ovan gjorda bedömningar (se avsnitt 12.3.3), att kunna omfattas av ett system för att verifiera identitet biometriskt mot handlingar.

Frågan är om det ytterligare bör preciseras vilka handlingar – inom ramen för ovan nämnda handlings*typer* – som bör kunna användas, men även om en större flexibilitet bör övervägas.

Vi bedömer i avsnitt 21.2 att en möjlighet för myndigheter att biometriskt verifiera identitet mot en handling, och begära att den enskilde gör handlingen tillgänglig för kontroll, behöver regleras i lag. Ett krav på att göra handlingen tillgänglig grundar sig – som vi återkommer till i nämnda avsnitt – dels på bestämmelser i tillämpliga EU-förordningar, dels på ett övergripande behov av tydlighet och förutsebarhet. Vi bedömer emellertid att möjligheterna till kontroll mot ovan nämnda typer av handlingar inte behöver begränsas i lag på så sätt att det framgår att endast vissa specifika hemlandspass eller identitetskort får användas. I stället bör det vara möjligt för regeringen – eller den eller de myndigheter regeringen bestämmer – att närmare specificera mot vilka sådana handlingar en kontroll ska kunna göras. En sådan lösning ger, enligt vår bedömning, tillräcklig förutsebarhet för den enskilde samtidigt som en viss flexibilitet bibehålls genom att det är möjligt för regeringen och – efter förordnande – myndigheter att tydliggöra och begränsa mot vilka handlingar en biometrisk verifieringen ska kunna göras såväl generellt, som i den myndighetsspecifika verksamheten. I det här avseendet kan en jämförelse göras med regelverket för identitetskontroll i folkbokföringsverksamheten. Skatteverket har bemyndigats att meddela närmare föreskrifter om vilka handlingar som ska godtas som pass, identitetskort eller motsvarande handling – enligt tillämpliga bestämmelser i folkbokföringslagen och lagen om samordningsnummer – och om hur identitetskontrollen ska genomföras. Av meddelade föreskrifter framgår bland annat att som pass godtas ett hemlandspass som är utfärdat av behörig myndighet i det land där

innehavaren är medborgare, och som identitetskort godtas ett identitetskort för EES-medborgare eller medborgare i Schweiz som är utfärdat av behörig myndighet i det land där innehavaren är medborgare.[37]

I syfte att främja en större flexibilitet skulle det även kunna övervägas att tillämpa någon form av generalklausul, exempelvis genom att det anges att en ”annan motsvarande handling” får användas, på motsvarande sätt som i Skatteverkets folkbokföringsverksamhet (se 26 b § folkbokföringslagen). Det skulle som vi ser det kunna argumenteras för att det inte på förhand alls bör begränsas vilka typer av handlingar som kan användas, utan att detta får avgöras utifrån vad som är praktiskt möjligt, det vill säga utifrån vilka typer av handlingar som vid en viss given tidpunkt innehåller biometriska underlag i digitalt format. Det skulle möjliggöra biometrisk verifiering mot typer av handlingar som eventuellt tillkommer i framtiden, utan att bestämmelser om biometrisk verifiering behöver justeras endast av den anledningen. En sådan ordning skulle emellertid kunna innebära ett betydande bedömningsutrymme för den breda krets av myndigheter som – enligt vår bedömning i avsnitt 21.3.1 – bör kunna få biometriskt verifiera identitet mot en handling. En möjlighet att genom föreskrifter definiera även vilka *typer* av handlingar som bör kunna användas är enligt vår bedömning inte lämpligt, med hänsyn till vad som ovan anförts angående behov av tydlighet och krav på stöd i lag. Det kan även antas att sådana föreskrifter kräver överväganden avseende lämpligheten av att en viss typ av handling får användas som inte går att göra på ett enkelt sätt.

Mot denna bakgrund anser vi att det inte bör vara möjligt att – inom ramen för ett mer generellt system för att biometriskt verifiera identitet mot en handling – använda andra typer av handlingar än de som nämnts ovan, i vart fall inte genom att detta bestäms i annan form än lag. Som vi nämnt inledningsvis i avsnitt 19.1 är denna bedömning inte avsedd att påverka eller inskränka befintliga och föreslagna möjligheter till sådana kontroller.

Den myndighet som vill biometriskt verifiera identitet, med stöd av det regelverk vi överväger, bör enligt vår mening kunna välja vilken eller vilka av de relevanta handlingarna som i ett enskilt ärende an-

[37] 2 kap. 2 och 3 §§ i både Skatteverkets föreskrifter om identitetskontroll hos Skatteverket (SKVFS 2023:5) och Skatteverkets föreskrifter om identitetskontroll vid tilldelning och förnyelse av samordningsnummer (SKVFS 2023:6).

vänds för kontrollen. Det bör alltså inte föreskrivas att en viss inbördes ordning bör gälla vid tillämpningen utan det ankommer på den kontrollerande myndigheten att, utifrån omständigheterna i det enskilda fallet, avgöra vilken typ av handling som bör användas. Med hänsyn till att det i första hand bör vara fråga om att stärka kopplingen till en identitet som har etablerats av svenska myndigheter kan det enligt vår mening dock finnas anledning för myndigheten att i första hand kräva att handlingar som är utfärdade av svenska myndigheter och som innehåller en individbeteckning görs tillgängliga för kontrollen, när detta är möjligt.

20 Allmänt om biometrisk verifiering av identitet mot handlingar

20.1 Inledning

I kapitel 19 har vi redogjort för vilka typer av handlingar som vi anser bör kunna användas för biometrisk verifiering, i ett system för säkrare verifiering av identitet som bör kunna tillämpas av en bredare krets myndigheter än de som i dag kan genomföra sådana kontroller. I kapitel 21 redogör vi för våra överväganden kring när biometrisk verifiering – såväl mot ett identitetsindex som mot handlingar – bör få användas. Vi anser emellertid att det är lämpligt att redan här – i likhet med kapitel 18 avseende ett system med ett identitetsindex – belysa vissa övergripande frågor som aktualiseras för ett system med säkrare verifiering av identitet, men som bygger på biometriska jämförelser mot handlingar. Bland annat behöver ställning tas till vilka typer av biometriska uppgifter som bör kunna användas, upptagning av biometriska underlag och hur dessa och de biometriska uppgifter som kan tas fram ur dem får behandlas efter att en kontroll har genomförts.

20.2 Biometriska uppgifter som bör få användas

Vår bedömning

Biometriska uppgifter som kan tas fram ur den ansiktsbild eller de fingeravtryck som är lagrade i en handling, eller som kan tas fram ur en synlig ansiktsbild på handlingen, bör få användas för att biometriskt verifiera identitet.

I avsnitt 11.4.5 har vi tagit ställning till vilka biometriska uppgifter som bör få lagras i ett identitetsindex, och då gjort bedömningen att ett index endast bör innehålla sådana uppgifter som kan tas fram ur en ansiktsbild. Vår bedömning att biometriska uppgifter från fingeravtryck inte också bör lagras i ett sådant system motiveras framför allt av integritetshänsyn och principen om uppgiftsminimering i dataskyddsförordningen, sett i ljuset av att vi anser att det inte finns ett utpräglat behov av att kunna använda två olika typer av biometriska uppgifter vid en verifiering eller identifiering mot ett identitetsindex. Frågan är om en annan bedömning bör göras avseende verifiering av identitet mot biometriska uppgifter i en handling.

Den yttre ramen för den nu aktuella bedömningen utgörs, som vi ser det, av vilken typ av biometriska underlag som finns på de handlingar som kan användas för jämförelsen, såväl digitalt i ett lagringsmedium som synligt på handlingen. Utifrån denna ram kan tillämplig rättslig reglering för en viss typ av handling tänkas begränsa vilka underlag som kan användas. Tekniska begränsningar kan också aktualiseras. Eftersom behandling av personuppgifter, inklusive känsliga sådana i form av biometriska uppgifter, kommer att utföras vid en biometrisk verifiering (se avsnitt 21.7) kan även det intrång i den personliga integriteten som detta kan medföra få betydelse.

20.2.1 Generella avgränsningar

Vi kan konstatera att de typer av handlingar som vi i kapitel 19 har bedömt bör kunna användas för biometrisk verifiering är försedda med ett lagringsmedium där biometriska underlag i form av både ansiktsbild och fingeravtryck är lagrade i digitalt format. De innehåller dessutom en synlig ansiktsbild av innehavaren. Det kan här förtydligas att det är biometriska *underlag* som lagras digitalt i ett chip på handlingarna, alltså inte de biometriska uppgifter som kan tas fram ur en ansiktsbild eller fingeravtryck.

Som vi redogjort för i avsnitt 11.4.5 kan det i de flesta fall visserligen antas vara tillräckligt att jämföra de biometriska uppgifter som kan tas fram ur endera en ansiktsbild eller fingeravtryck för att verifiera någons identitet. Samtidigt kan en kontroll av flera typer av biometriska uppgifter i åtskilliga situationer innebära en större säkerhet än vad som skulle vara fallet om underlaget var mer begränsat,

till exempel när den som ska kontrolleras har allvarliga skador i ansikte eller på händerna eller om tekniska problem inte möjliggör att endera biometriskt underlag kan tas upp.[1] I promemorian *Ökad säkerhet för vissa identitets- och uppehållshandlingar – anpassning av svensk rätt till en ny EU-förordning* lyftes exempelvis fram att ”verifieringen blir betydligt säkrare om inte bara fotografi utan även fingeravtryck får tas och jämföras.”[2] Med hänsyn till detta, och mot bakgrund av att vårt uppdrag i grunden syftar till att möjliggöra en mer tillförlitlig verifiering av identitet i fler situationer än i dag, framstår det inte som ändamålsenligt att mer allmänt begränsa vilka biometriska underlag som får användas; både ansiktsbild och fingeravtryck lagras på de aktuella handlingarna just i syfte att möjliggöra en säkrare kontroll av innehavarens identitet. Möjligheten att verifiera identiteten med biometriska uppgifter vid ett visst givet tillfälle bör inte i praktiken vara avhängig exempelvis av om utrustning för att ta upp antingen fingeravtryck eller ansiktsbild är ur funktion. Vi kan vidare konstatera att gällande och föreslagna bestämmelser som gör det möjligt att genomföra en kontroll av biometriska underlag i olika handlingar – exempelvis 9 kap. 8 b § utlänningslagen (2005:716), 26 c § folkbokföringslagen (1991:481) och förslaget till 13 f § i lagen (2001:82) om svenskt medborgarskap – inte i något fall innehåller en begränsning till antingen ansiktsbild eller fingeravtryck (se även avsnitt 7.4.2).

Mot denna bakgrund anser vi att utgångspunkten bör vara att biometriska uppgifter som kan tas fram från både ansiktsbild och fingeravtryck bör få användas för att verifiera identiteten mot en handling.

20.2.2 Rättsliga begränsningar

Vilka biometriska underlag som får användas i de typer av handlingar som vi i kapitel 19 har bedömt bör omfattas av en utökad möjlighet att kontrollera biometriska uppgifter mot, begränsas vad gäller myndigheter inte i någon av de tillämpliga EU-förordningarna. Av artikel 4.3 i passförordningen[3] framgår att de ”biometriska kännetecknen” i pass och resehandlingar får användas för kontroll och av artikel 11.6

[1] Jfr *Folkbokföringsverksamhet, biometri och brottsbekämpning,* SOU 2025:75, s. 424.
[2] Ds 2020:22, s. 78.
[3] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004.

och 11.7 i EU:s id-kortsförordning[4] framgår att såväl ansiktsbild som fingeravtryck får användas av myndigheter, under förutsättning att övriga rekvisit i artikel 11 är uppfyllda. Enligt artikel 11.7 c får däremot tillgång till fingeravtryck endast ges till myndigheter. När det gäller uppehållstillståndskort anges i artikel 4 i EU-förordningen om en enhetlig utformning av uppehållstillstånd[5] att de ”biometriska kännetecknen” i uppehållstillstånd får användas för kontroll av innehavarens identitet. Inte heller i övrigt har vi funnit att det finns några rättsliga hinder mot att myndigheter använder både den ansiktsbild och de fingeravtryck som har lagrats i chippet på en handling som jämförelsematerial vid en sådan kontroll. Vi kan notera att i skäl 18 till EU:s id-kortsförordning fastställs en prioritetsordning för sätten att kontrollera en handlings äkthet och innehavarens identitet. Där anges nämligen att medlemsstaterna ” i första hand [ska] kontrollera ansiktsbilden och, om det behövs för att med säkerhet bekräfta handlingens äkthet och innehavarens identitet, även kontrollera fingeravtrycken” (jfr EU-domstolens dom i målet C-61/22, *Landeshauptstadt Wiesbade*n, p. 117). Det innebär enligt vår mening emellertid inte att det finns ett hinder mot att möjliggöra att båda typer av underlag får användas, utan tvärtom att det finns stöd för detta.

20.2.3 Tekniska faktorer

För att de biometriska underlag som finns lagrade digitalt i en viss handling ska kunna användas vid en verifiering förutsätts att myndigheten tekniskt har tillgång till dem. Vad gäller fingeravtryck är de vanligtvis krypterade på ett sådant sätt att de endast kan kontrolläsas efter avtal med det land som utfärdat handlingen. För att kunna ta fram fingeravtryck från ett lagringsmedium i ett utländskt pass eller identitetskort behövs ett certifikat från det utfärdande landet. Det kan därmed krävas att varje svensk myndighet som vill få tillgång till certifikaten dels sluter avtal med varje utfärdandeland, dels administrerar förnyelse av varje enskilt certifikat när det löper ut. Polismyndigheten har ingått sådana avtal.[6] I betänkandet Folkbokföringsverksamhet, biometri och brottsbekämpning anfördes, i fråga om Skatteverket, att myndigheten bedömt att den inte utför några kon-

[4] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.
[5] Rådets förordning (EG) nr 1030/2002 av den 13 juni 2002.
[6] *En säker och tillgänglig statlig e-legitimation,* SOU 2023:61, s. 168.

troller av fingeravtryck på grund av avsaknad av certifikat; även om Skatteverket skulle kunna få certifikat från Polismyndigheten för svenska pass och nationella identitetskort för att kontrollera fingeravtryck som lagras i dessa, bedömde Skatteverket att nyttan av att kontrollera fingeravtryck i enbart svenska handlingar inte vägs upp av kostnaderna för certifikat och den förnyelseadministration som skulle krävas var trettionde dag för att det skulle vara möjligt.[7]

Möjligheten för myndigheter att i praktiken använda biometriska underlag i form av fingeravtryck vid en verifiering mot en viss handling kan alltså vara starkt begränsad med hänsyn till tekniska skäl av nyss nämnda slag. Vi anser emellertid att det inte utgör anledning att begränsa möjligheten rättsligt. Andra myndigheter än Skatteverket kan göra en annan bedömning av behovet av att kunna verifiera identiteten med hjälp av fingeravtryck, och bör då kunna ingå nödvändiga avtal för att få tillgång till de certifikat som krävs för att ta fram sådana biometriska underlag. Motsvarande begränsningar i fråga om certifikat finns inte för den ansiktsbild som finns på lagringsmediet, eller är synlig på handlingen. Tekniska begränsningar på så sätt att två olika typer av underlag kräver större lagringskapacitet än om endast en typ används gör sig inte gällande på samma sätt som i ett identitetsindex av det slag som vi redogjort för i kapitel 11–18.

En typ av teknisk begränsning kan hänföras till det sätt som verifieringen bör få genomföras på; en biometrisk verifiering bör som vi ser det även kunna genomföras på distans, till exempel genom att innehavaren av handlingen använder en mobiltelefon för att ta upp biometriska underlag som kan användas för en jämförelse med uppgifter som är lagrade i ett chip på handlingen (se avsnitt 27.4). Fingeravtryck som läses med hjälp av en inbyggd sensor i en mobiltelefon lagras inte som en bild, utan som en krypterad biometrisk mall i en säker del av mobilenheten. Operativsystemet tillhandahåller ett API (programgränssnitt) – exempelvis Touch ID på en iPhone – som låter en tredjepartsapplikation fråga om autentisering, men inte läsa själva fingeravtrycket eller den biometriska mallen som tas fram ur det. Systemet ger alltså endast svar i form av om autentiseringen lyckades eller misslyckades. Detta är en säkerhetsåtgärd för att förhindra identitetsstöld och missbruk av biometriska uppgifter. Detta innebär att det inte är möjligt att använda en inbyggd sensor för fingeravtryck på en mobiltelefon för att ta fram biometriska upp-

[7] SOU 2025:75, s. 385.

gifter som kan jämföras med de som kan tas fram ur chippet på den handling som ska användas för verifieringen; de biometriska underlag som tas upp kan endast jämföras med de som är lagrade i en säker del av enheten. Att med hjälp av kameran i mobiltelefonen fotografera innehavarens fingeravtryck för att ta fram biometriska uppgifter ur den, som har en tillräcklig kvalitet, är inte heller möjligt.

Även om det med nuvarande tekniska lösningar inte är möjligt att ta upp biometriska underlag i form av fingeravtryck på distans utgör det enligt vår mening inte skäl att helt utesluta en potentiell användning av dem. Det kan också vara möjligt att ta upp fingeravtryck vid personlig inställelse, genom att särskild utrustning för detta används, på liknande sätt som redan görs vid exempelvis en ansökan om pass eller en gränskontroll.

Några tekniska begränsningar i övrigt som talar mot att både ansiktsbild och fingeravtryck bör få användas vid en verifiering har vi inte kunnat finna.

20.2.4 Underlag i form av en synlig ansiktsbild

Som vi konstaterat ovan innehåller samtliga typer av handlingar som vi i kapitel 19 har ansett bör kunna användas vid biometrisk verifiering även en synlig ansiktsbild av innehavaren. Det är möjligt att ta fram biometriska uppgifter från denna bild, även om tillförlitligheten i underlaget kan antas vara lägre än för den digitala ansiktsbild som är lagrad på handlingen. Biometriska uppgifter som kan tas fram på detta sätt får däremot för närvarande inte användas vid en kontroll enligt exempelvis 9 kap. 8 b § utlänningslagen och 26 c § folkbokföringslagen. I propositionen *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten* har emellertid förslag lämnats om att Skatteverket ska ges en sådan möjlighet.[8] Detta mot bakgrund av uttalanden i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* om att det möjliggör en kontroll av biometriska uppgifter vid fler identitetskontroller än för närvarande, eftersom det är möjligt att förstöra ett lagringsmedium på en identitetshandling eller ett uppehållstillståndskort och att kontrollen då kan göras mot två skilda källor på handlingen. I betänkandet konstaterades även

[8] Prop. 2025/26:261, s. 52 f.

att det inte är ovanligt att ett lagringsmedium inte kunnat läsas vid de identitetskontroller som görs av Skatteverket.[9]

För det fall myndigheter ges en bredare möjlighet att använda biometriska uppgifter för att verifiera identitet mot handlingar anser vi att det är av vikt att detta faktiskt kan genomföras i så många fall som möjligt, när det finns ett rättsligt stöd för det. Att kunna använda flera potentiella biometriska underlag är ett betydelsefullt led i att främja detta. Vi anser därför att biometriska uppgifter som kan tas fram ur en synlig ansiktsbild på en handling också bör kunna användas. Denna metod kan dock, som vi ser det, i första hand komma att användas vid personlig inställelse, inte på distans. Detta eftersom det normalt inte är möjligt för myndigheten att på distans säkerställa att den ansiktsbild som används som källa för de biometriska uppgifterna faktiskt härrör från en viss typ av handling och inte från någon annan källa.

20.2.5 Integritetsaspekter

Lagring av ansiktsbild och fingeravtryck och de biometriska uppgifter som kan tas fram ur dessa i ett identitetsindex skulle medföra behandling av två olika typer av biometriska underlag och biometriska uppgifter för en potentiellt stor mängd personer. De överväganden vi gjort i avsnitt 11.4.5 bör dock ses i ljuset av att det i ett identitetsindex dels är fråga om lagring av uppgifter, dels att indexet – enligt vad vi anfört i kapitel 18 – bör kunna användas inte bara för verifiering av identitet utan även i vissa fall för identifiering, vilket innebär att en stor mängd känsliga personuppgifter behöver behandlas i samband med en sådan en-till-många-jämförelse. Att vid sådana förhållanden så långt som möjligt begränsa vilka uppgifter som behandlas har enligt vår mening en helt annan tyngd än vid en sådan momentan behandling som utförs vid verifiering av identitet mot handlingar, det vill säga en en-till-en-jämförelse (se avsnitt 21.7 angående personuppgiftsbehandling).

Vid verifiering mot handlingar anser vi att vikten av att kunna verifiera identitet i så många fall som möjligt i stället bör vara av avgörande betydelse. Integritetsaspekter utgör därför inte skäl för att endast biometriska underlag i form av ansiktsbild bör få användas.

[9] SOU 2025:75, s. 420 f.

20.3 Upptagning av biometriska underlag

Vår bedömning

Det bör inte regleras i författning hur biometriska underlag ska tas upp vid biometrisk verifiering av identitet mot handlingar, exempelvis genom ett uttryckligt krav på personlig inställelse.

Vi har i avsnitt 18.3.2 bedömt att det vid verifiering av identitet mot ett identitetsindex inte bör regleras i författning hur en ansiktsbild som används för den biometriska jämförelsen ska tas upp, exempelvis genom ett krav på personlig inställelse. Vi anser att de omständigheter som vi redogjort för i nämnda avsnitt gör sig gällande även vid verifiering mot handlingar och hänvisar därför i allt väsentligt till de överväganden vi gjort i nämnda avsnitt, med följande tillägg.

Vi har i avsnitt 20.2 bedömt att även fingeravtryck bör få användas vid biometrisk verifiering av identitet mot handlingar. Att sådana biometriska underlag, med nuvarande teknik, inte kan tas upp på distans på ett tillförlitligt eller användbart sätt skulle visserligen kunna anses tala för att reglera hur upptagningen av biometriska underlag bör gå till vid biometrisk verifiering av identitet mot handlingar, och eventuellt ett krav på personlig inställelse; möjligheterna till biometrisk verifiering stärks om både ansiktsbild och fingeravtryck kan användas. Det får emellertid anses stå klart att det normalt är tillräckligt att en typ av biometriskt underlag kan tas upp för att kunna genomföra en biometrisk verifiering. Att upptagning av fingeravtryck – åtminstone med nuvarande tekniska möjligheter – endast kan göras vid personlig inställelse utgör därför inte ett skäl att reglera att upptagning av biometriska underlag *alltid* ska ske genom personlig inställelse.

De tekniska förutsättningarna vid en viss given tidpunkt och karaktären på det ärendeslag där en biometrisk verifiering genomförs bör som vi ser det i stället vara styrande, för att möjliggöra en flexibel och därmed effektiv tillämpning av ett system för att biometriskt verifiera identitet mot handlingar. Det är enligt vår mening inte heller möjligt att, för den breda krets av myndigheter som vi anser bör kunna omfattas (se avsnitt 21.3.1), på förhand avgöra om de kommer att ha en faktisk möjlighet att göra sådana kontroller vid personlig inställelse. Det skulle därför medföra svårigheter när det gäller tillämpningsområdet för en eventuell reglering kring sättet för hur de bio-

metriska underlagen bör tas upp. Att reglera detta för endast vissa myndigheter är inte heller lämpligt. Som vi anfört i avsnitt 18.3.2 anser vi även att det är sannolikt att den tekniska utvecklingen möjliggör att en ansiktsbild tas upp på distans, exempelvis genom att den enskilde själv – med hjälp av en applikation på sin mobiltelefon – tar en bild av sitt ansikte, som kan användas för verifiering av identitet (i kapitel 27 ger vi en översiktlig teknisk beskrivning av hur detta kan gå till, med befintlig teknik). Inte heller i övrigt anser vi att det kommit fram några omständigheter som talar för ett behov av att uttryckligen reglera *hur* en myndighet tar upp de biometriska underlag som används för biometrisk verifiering mot handlingar. I kapitel 23 återkommer vi till frågan om myndigheter bör få möjlighet att, som ett led i att kunna verifiera identitet biometriskt mot en handling, kräva att den vars identitet ska kontrolleras inställer sig personligen.

20.4 Begränsning till barn över sex år

Vår bedömning

En möjlighet att biometriskt verifiera identitet mot handlingar på det sätt som vi överväger bör inte gälla för barn under sex år.

En fråga att ta ställning till är om en möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar bör omfatta barn, det vill säga personer som inte har fyllt 18 år. Vi har tidigare bedömt att barn inte generellt bör undantas från registrering i ett identitetsindex, men att det saknas behov av att registrera barn som inte har fyllt sex år (se avsnitt 12.4.1). Vi gör motsvarande bedömning vad gäller en möjlighet att verifiera identitet biometriskt mot handlingar, och beaktar då i stor utsträckning samma omständigheter som vi redogjort för i fråga om ett identitetsindex.

Även om det naturligtvis inte sker i samma utsträckning som för vuxna kan det finnas ett behov av att verifiera identitet för ett barn i olika sammanhang. Vidare syftar möjligheten att verifiera identitet biometriskt mot handlingar inte bara till att möjliggöra utökad kontroll, utan också till att motverka att enskilda får sina identiteter utnyttjade utan deras vetskap, vilket är ett allt större problem. Barn kan var särskilt utsatta i sådana sammanhang. Med hänsyn till detta

bör barn inte generellt sett undantas. Det saknas dock anledning att låta myndigheter verifiera identiteten biometriskt mot handlingar för barn som inte har fyllt sex år. För så små barn kan det nämligen endast i undantagsfall antas finnas ett behov av att verifiera identitet. Enligt vår bedömning bör möjligheten att verifiera identitet biometriskt mot handlingar därmed inte gälla för barn under sex år.

Det kan påpekas att det även för barn över sex år sällan kan antas finnas ett behov av att biometriskt verifiera identiteten. Det kommer oftast att vara tillräckligt för en myndighet att – vid behov av att kontrollera identitet – verifiera vårdnadshavarens eller vårdnadshavarnas identitet. För de situationer där det i undantagsfall finns ett behov av att verifiera identiteten mot handlingar för ett barn över sex år bör myndigheterna dock ha en sådan möjlighet. En annan sak är att det inte är ovanligt att yngre barn saknar handlingar som gör det möjligt att genomföra en biometrisk verifiering. Uppehållstillståndskort utfärdas dock regelmässigt till alla barn vid beviljande av uppehållstillstånd med längre giltighetstid än sju dagar. Det kan också antas vara relativt vanligt att barn under sex år har ett giltigt hemlandspass.

20.5 Uppgifter som en myndighet bör få tillgång till vid biometrisk verifiering mot handlingar

Vår bedömning

Den myndighet som verifierar en persons identitet biometriskt mot en handling behöver få tillgång till uppgifter om resultatet av den biometriska jämförelsen samt de identitetsuppgifter och eventuell identitetsbeteckning som hämtats ur lagringsmediet i den handling som använts för verifieringen.

I kapitel 27 beskriver vi hur en verifieringsprocess för att biometriskt verifiera identitet mot handlingar som bygger på ett system med en myndighets egna system (avsnitt 27.3), respektive ett system med myndighetsgemensamma komponenter (avsnitt 27.4) kan vara uppbyggt. Tanken är att myndigheter framför allt ska kunna genomföra sådana kontroller på distans, genom att den vars identitet kontrolleras använder en mobilapplikation för att ta en ansiktsbild av sig

själv som kan användas för en biometrisk jämförelse mot den ansiktsbild som finns på ett lagringsmedium på en handling som han eller hon innehar. I detta avseende bör det, som vi ser det, bli aktuellt med en myndighetsgemensam teknisk lösning, vilken som utgångspunkt består av en mobilapplikation och ett så kallat backend-system. Tyngdpunkten för verifieringslogiken bör, utifrån nu tillgänglig teknik, finnas i backend-systemet (se avsnitt 27.6). Efter att den biometriska jämförelsen har genomförts – enligt den modell vi beskriver i avsnitt 27.4.1 – ska backend-systemet skicka ett svar till den myndighet som bestämt att verifieringen ska genomföras. Svaret ska kunna innehålla dels resultatet av den biometriska jämförelsen (PASS/FAIL eller ett jämförelsevärde[10]), dels identitetsuppgifter och, om en sådan finns lagrad i handlingen, identitetsbeteckning. Som vi nämnt i avsnitt 19.3.3 innehåller uppehållstillståndskort som utfärdas av Migrationsverket inte det unika individnummer som myndigheten tilldelar sökanden; svaret från ett backend-system kan därför inte innehålla denna typ av uppgift.

Vid ett införande av ett system som möjliggör biometrisk verifiering mot handlingar genom en myndighetsgemensam teknisk lösning kommer sannolikt en annan myndighet än den som bestämt att en sådan kontroll ska genomföras att vara ansvarig för den tekniska lösningen, inklusive backend-systemet (se kapitel 29). Utgångspunkten är att backend-systemet bör utformas så att det finns administrativa och/eller tekniska begränsningar som gör att den myndighet som kan komma att ansvara för backend-systemet inte kan ta del av uppgifterna i läsbart skick. Det ska inte heller lagras några personuppgifter i backend-systemet utan det ska, något förenklat, fungera endast som en förmedlare av information mellan mobilapplikationen och den myndighet som vill genomföra en biometrisk verifiering.

Om den biometriska jämförelsen lyckas behöver av naturliga skäl uppgift om resultatet av den biometriska jämförelsen samt de identitetsuppgifter och eventuell identitetsbeteckning som hämtats ur lagringsmediet i den handling som använts för verifieringen vara tillgängliga för den myndighet som bestämde att verifieringen skulle genomföras i det enskilda fallet, genom att de på lämpligt tekniskt sätt hämtas från backend-systemet till myndighetens egna system (se avsnitt 27.4.2 avseende vilka systemkomponenter som kan behöva

[10] Ett jämförelsevärde är det numeriska värde som systemet beräknar för att avgöra likheten mellan de biometriska uppgifterna som används vid jämförelsen.

utvecklas i detta syfte). Myndigheten kan då jämföra dessa med uppgifter om identitet m.m. som hänför sig till den påstådda identiteten. Stämmer även dessa kan identiteten anses ha verifierats och myndigheten har fått svar på frågan om personen är den som han eller hon utger sig för att vara.

Om den biometriska jämförelsen i stället medför en misslyckad matchning behöver givetvis en uppgift om detta kunna göras tillgänglig för den myndighet som bestämde att den biometriska verifieringen skulle genomföras. Att jämförelsen misslyckades kan som vi ser det bero antingen på att den enskilde försökt använda en identitetshandling som är utfärdad eller ett uppehållstillståndskort som är utfärdat för någon annan, eller på tekniska problem, exempelvis att kameran på den mobilenhet som den enskilde har använt inte är tillräckligt bra eller skadad. Den enskilde kan också tänkas ha fysiska skador som medför att biometriska underlag av tillräcklig kvalitet inte kan tas upp. Oavsett anledningen anser vi att det även i dessa fall kan vara av värde för myndigheten att uppgifter om identiteten och eventuell identitetsbeteckning som är lagrade i den handling som användes kan göras tillgängliga. Utifrån uppgifterna bör det vara enklare för myndigheten att ta ställning till vilka vidare utredningsåtgärder som eventuellt bör eller kan vidtas i det enskilda fallet, exempelvis om någon annan metod kan användas för att verifiera identitet i det enskilda fallet, eller om kontakt bör tas med den enskilde för att kontrollera anledningen till att den biometriska verifieringen inte lyckades. En misslyckad matchning behöver inte nödvändigtvis utgöra ett försök att vilseleda utan kan i stället bero på tekniska faktorer i det enskilda fallet. Om matchningen har misslyckats och de identitetsuppgifter som görs tillgängliga inte stämmer med de som den enskilde uppgett för myndigheten är det emellertid en tydlig indikation på att någon form av identitetsmissbruk är för handen. Vetskap om att myndigheten får tillgång till uppgifterna i den handling som den enskilde använder för att biometriskt verifiera sin identitet kan också verka förebyggande i viss mån; det går exempelvis inte att använda någon annans identitetshandling och samtidigt påstå att en korrekt handling har använts. Sådana försök kan då motverkas. Vi anser även att det kan finnas ett värde för den enskilde att myndigheten kan göra korrekta avvägningar, särskilt om det finns tekniska anledningar till att den biometriska jämförelsen inte lyckades.

Sammanfattningsvis behöver den myndighet som verifierar en persons identitet biometriskt mot en handling få tillgång till uppgifter om resultatet av den biometriska jämförelsen samt de identitetsuppgifter och eventuell identitetsbeteckning som hämtats ur lagringsmediet i den handling som använts för verifieringen. Vi återkommer i avsnitt 24.12 till frågor om elektronisk åtkomst och utlämnande av personuppgifter samt i kapitel 25 till frågor om sekretess.

20.6 Efterföljande behandling av biometriska underlag och biometriska uppgifter

Vår bedömning

Ansiktsbild och fingeravtryck som tagits upp i syfte att biometriskt verifiera identitet mot en handling, med stöd av ett sådant regelverk som vi överväger, bör omedelbart förstöras efter att kontrollen har genomförts. Detsamma bör gälla för de biometriska uppgifter som har tagits fram ur ansiktsbilden och fingeravtrycken samt ur de biometriska underlagen i den handling mot vilken verifieringen har genomförts.

En möjlighet för myndigheter att använda biometrisk verifiering av identitet mot handlingar, på det sätt vi överväger, bör enligt våra övervägandet i avsnitt 21.5 endast få användas i väl avgränsade situationer, och syftar till att myndigheter vid behov ska kunna verifiera identitet på ett säkert sätt. Någon omständighet som motiverar att ansiktsbild eller fingeravtryck som tagits upp i syfte att biometriskt verifiera identitet mot en handling fortsatt ska få behandlas av den myndighet som har bestämt att verifieringen ska genomföras även efter att kontrollen har genomförts har vi inte funnit. Under alla omständigheter är det inte lämpligt att inom ramen för vårt uppdrag möjliggöra att myndigheter som enligt vår bedömning bör få verifiera identitet mot en handling med hjälp av biometriska uppgifter kan bygga upp egna register utifrån de biometriska underlag som tagits upp i detta syfte.

Vi anser därför att de biometriska underlag som tagits upp från den enskilde och de biometriska uppgifter som tagits fram ur dessa, för att möjliggöra verifieringen, omedelbart ska förstöras efter att

kontrollen har genomförts. Detsamma gäller de biometriska uppgifter som tagits fram ur underlagen i den handling mot vilken verifieringen genomförs. Genom dessa skyddsåtgärder begränsas behandlingen av ansiktsbilder och fingeravtryck och de biometriska uppgifter som har tagits fram ur dem.

21 Användning av biometrisk verifiering

21.1 Inledning

Vi har i kapitel 11–20 beskrivit de rättsliga förutsättningarna för att på olika sätt främja en stärkt verifiering av identitet med hjälp av biometriska uppgifter, som bygger på en jämförelse antingen mot uppgifter i ett centralt register i form av ett identitetsindex eller i handlingar av olika slag. Nämnda kapitel innehåller bedömningar av de grundläggande förutsättningarna för respektive system. Vi behöver emellertid också närmare redogöra för hur de olika systemen bör kunna användas. Som utgångspunkt bör en utökad möjlighet att använda biometriska uppgifter för att verifiera identitet – oavsett vilket av de två system vi överväger som är aktuellt – främja att fler aktörer än i dag kan ta del av information bland annat om de identiteter som har etablerats av Polismyndigheten, Migrationsverket och Skatteverket. En annan viktig utgångspunkt är att en sådan verifiering av identitet bör kunna användas i många olika ärendeslag och situationer. En särskild fråga är om en utökad möjlighet till biometrisk *verifiering* bör kunna användas i brottsbekämpande verksamhet. Detta tar vi ställning till i avsnitt 21.4; i avsnitt 18.3.1 har vi belyst möjligheten att använda ett identitetsindex för *identifiering* i brottsbekämpande verksamhet. En ambition att utöka möjligheten till biometrisk verifiering måste också ta i beaktande de risker som den till verifieringen kopplade behandlingen av biometriska uppgifter och andra personuppgifter kan innebära, och det integritetsintrång som behandlingen kan medföra för den enskilde. Relevanta EU-förordningar måste också beaktas. Begränsningar i användningen behöver därför övervägas, exempelvis när en sådan metod för att verifiera identitet bör få användas, och av vilka aktörer. I detta kapitel tar vi ställning till dessa frågor.

21.2 Användningen behöver regleras i lag

Vår bedömning

En generell möjlighet för myndigheter att på det sätt vi överväger biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar behöver regleras i lag.

Som vi återkommer till i avsnitt 21.7 innebär verifiering av identitet mot handlingar med hjälp av biometriska uppgifter ett visst intrång i skyddet för den personliga integriteten som följer av regeringsformen, Europakonventionen[1] och EU:s rättighetsstadga[2]. Detta bland annat med hänsyn till att biometriska underlag behöver tas upp för att möjliggöra en sådan kontroll och att biometriska uppgifter som kan tas fram ur underlagen behöver behandlas av den myndighet som genomför kontrollen, även om matchningen görs i ett backend-system (se avsnitt 27.4 för en teknisk beskrivning av en möjlig verifieringsprocess). Även vid biometrisk verifiering mot ett identitetsindex behöver biometriska underlag tas upp, och vi har i avsnitt 16.5.3 bedömt att verksamheten med ett identitetsindex, men även användningen av ett sådant system, bör regleras i lag. Integritetsintrånget för enskilda får visserligen anses betydligt mindre vid verifiering mot handlingar än vid registrering i ett index som potentiellt kan komma att innehålla uppgifter om flera miljoner personer. En möjlighet för en bred krets av myndigheter att i varierande ärendeslag och verksamhetsslag biometriskt verifiera identitet måste emellertid, enligt vår mening, präglas av tydlighet och förutsebarhet. Detta kan främjas bland annat genom att det noggrant övervägs och tydligt avgränsas under vilka förutsättningar sådana kontroller får genomföras (se avsnitt 21.5). Det rättsliga stödet behöver dock även vara på en normgivningsnivå som inte medger att det lätt kan utökas på sätt som medför ökade risker för den personliga integriteten, som inte är avsedda. Redan detta talar enligt vår mening med styrka för att en möjlighet för myndigheter att, på det sätt vi överväger, biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar behöver regleras i lag.

[1] Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[2] Europeiska unionens stadga om de grundläggande rättigheterna.

Vid biometrisk verifiering mot vissa av de typer av handlingar som vi i kapitel 19 har bedömt bör kunna användas, följer även krav på stöd i lag direkt av relevanta EU-förordningar. En förutsättning för att en myndighet ska kunna genomföra en biometrisk verifiering mot en viss handling är att myndigheten har möjlighet att begära att den enskilde gör handlingen tillgänglig för kontroll. När det gäller *hemlandspass* som utfärdas till svenska medborgare regleras dessa i EU:s passförordning.[3] Användningen av pass och resehandlingar för att biometriskt verifiera innehavarens identitet regleras i artikel 4.3 b i passförordningen. Av bestämmelsen följer att biometriska kännetecken i pass endast får användas för att kontrollera innehavarens identitet genom direkt tillgängliga jämförbara kännetecken när uppvisande av handlingen krävs enligt lag. Sådana bestämmelser finns exempelvis i 5 a § passlagen (1978:302), vid utresa från eller inresa till Sverige, men även i 9 kap. 8 c § utlänningslagen (2005:716). För det statliga identitetskort med resefunktion som föreslagits i promemorian Ett statligt identitetskort (Ju2026/01595) framgår en motsvarande reglering av artikel 11.6 b i EU:s id-kortsförordning[4]; att det i sistnämnda bestämmelse anges att ett krav på uppvisande ska framgå av lag ”eller annan författning” utgör enligt vår bedömning inte någon skillnad. Även för handlingar i form av *uppehållstillståndskort* som utfärdats av Migrationsverket framgår att krav på att visa upp en sådan handling för kontroll av de biometriska underlag som lagras i handlingen ska framgå av nationell lagstiftning (se artikel 4 i EU-förordningen om en enhetlig utformning av uppehållstillstånd[5]). Exempel på sådana bestämmelser är 9 kap. 8 b § utlänningslagen och 26 b § andra stycket folkbokföringslagen (1991:481). För flera av de typer av handlingar som vi anser att en biometrisk verifiering bör kunna genomföras mot (se avsnitt 19.3) följer det alltså av EU-förordningar att det ska vara uttryckligen angivet i nationell rätt att en myndighet får kräva att handlingen visas upp.

När det gäller statliga identitetskort *utan* funktion som resehandling omfattas dessa inte av EU:s id-kortsförordning; av skäl 13 till förordningen framgår att identitetshandlingar som utfärdas till medborgare vars rätt till fri rörlighet har begränsats i enlighet med unionsrätten eller nationell rätt och på vilka det uttryckligen anges att de

[3] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004.
[4] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.
[5] Rådets förordning (EG) nr 1030/2002 av den 13 juni 2002.

inte kan användas som resehandlingar inte bör anses omfattas av förordningen. Vidare uttalas det i promemorian *Ett statligt identitetskort* att EU:s id-kortsförordning inte gäller för statliga identitetskort utan funktion som resehandling.[6] Identitetskort som utfärdats av behörig myndighet i tredje land bör, enligt vår bedömning, som utgångspunkt även kunna användas för biometrisk verifiering. Några krav i regelverk som styr utfärdande av sistnämnda typer av handlingar, som innebär att det behöver vara uttryckligen angivet i svensk rätt att en myndighet får kräva att handlingen visas upp, har vi inte funnit. Även om det alltså saknas krav på stöd i lag anser vi – mot bakgrund av de integritetsaspekter som pekats på ovan – att det saknas anledning att ha någon annan utgångspunkt avseende dessa handlingar.

I avsnitt 20.2 har vi bedömt att biometrisk verifiering mot handlingar bör kunna genomföras med hjälp av såväl ansiktsbild som fingeravtryck. Att ta någons fingeravtryck är ett sådant kroppsligt ingrepp som omfattas av skyddet i bestämmelsen i 2 kap. 6 § första stycket regeringsformen. För att skyddet i nämnda bestämmelse ska få inskränkas krävs lagstöd.[7]

Vid en sammantagen bedömning av det ovan anförda anser vi att en generell möjlighet för myndigheter att på det sätt vi överväger i detta kapitel biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar behöver regleras i lag.

21.3 Aktörer som bör omfattas

En första avgränsning som vi behöver ta ställning till är vilka aktörer som bör kunna omfattas av en utökad möjlighet att biometriska verifiera identitet, antingen mot ett identitetsindex eller mot handlingar. Även om utgångspunkten är att en så bred krets som möjligt bör omfattas kan vi konstatera att olika samhällsaktörer kan ha väsentligt olika förutsättningar – exempelvis i fråga om behov av att säkert verifiera identitet i sin verksamhet, organisation, rättslig styrning och ekonomiska incitament – som kan ha betydelse för om de bör omfattas av en generell möjlighet att biometriskt verifiera identitet. De två huvudgrupper som aktualiseras är som vi ser det myndigheter respektive privata aktörer.

[6] Ju2026/01595, s. 67.
[7] Se exempelvis *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll*, SOU 2024:80, s. 453.

21.3.1 Myndigheter

Vår bedömning

Myndigheter – med vilket avses de organ som ingår i den offentligrättsliga statliga eller kommunala organisationen – bör omfattas av en ny lag som reglerar en generell möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

Riksdagen och beslutande kommunala församlingar, de organ som anges i bilagan till offentlighets- och sekretesslagen (2009:400) samt bolag, föreningar och stiftelser där kommuner eller regioner utövar ett rättsligt bestämmande inflytande bör i detta avseende inte jämställas med myndigheter.

Det övergripande syftet med en utökad möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar är att motverka identitetsmissbruk, som bland annat riktar sig mot välfärdssystemen. Det framstår därför som givet att sådana system som utgångspunkt bör få användas av myndigheter för att säkert verifiera identitet. Frågan är dock om det finns anledning att begränsa användningen endast till vissa myndigheter; vi kan notera att biometrisk verifiering av identitet enligt gällande rätt är förbehållet en mycket snäv krets – i första hand Polismyndigheten, Skatteverket och Migrationsverket. Fråga är även om det finns aktörer som bör jämställas med myndigheter.

Samtliga myndigheter bör kunna omfattas

I början av år 2026 fanns det mer än 350 myndigheter under regeringen. Antalet kommunala myndigheter varierar eftersom varje kommun själv bestämmer hur många myndigheter den ska ha utifrån organisation och behov. Det finns 290 kommuner och med hänsyn till hur dessa vanligtvis organiserar sig därmed ett betydligt större antal kommunala myndigheter än statliga. Att tillåta endast statliga myndigheter att använda ett system för biometrisk verifiering av identitet skulle begränsa användningen betydligt. Kommunerna har emellertid en omfattande verksamhet inom ett flertal olika områden, och tar till exempel ställning till tillstånd att sälja tobak och till serveringstillstånd, men även till bistånd av olika slag. Det är därför en-

ligt vår mening angeläget att även kommunala myndigheter, som utgångspunkt, har möjlighet att verifiera identitet genom en kontroll mot ett index eller mot handlingar. Annars utesluts en stor andel av de offentliga aktörerna från möjligheten att säkert verifiera identitet, och ett system för detta skulle bli betydligt mindre effektivt som ett verktyg mot identitetsmissbruk mot det allmänna.

Vi kan i detta sammanhang notera att det av artikel 11.6 i EU:s id-kortsförordning framgår att endast *behöriga nationella myndigheter* får kontrollera identitet mot handlingar som utfärdats i enlighet med förordningen. Varken EU:s passförordning eller EU:s förordning om en enhetlig utformning av uppehållstillstånd innehåller någon motsvarande reglering. Vad som avses med uttrycket behöriga nationella myndigheter i id-kortsförordningen anges inte i förordningen. Det framgår inte heller att behöriga nationella myndigheter ska ges något särskilt ansvar eller utföra särskilda uppgifter som är förbehållna vissa myndigheter, exempelvis på det sätt som framgår avseende vilka myndigheter som enligt VIS-förordningen8 är behöriga att ha åtkomst till Schengens informationssystem för viseringar; av artikel 3.1.3–3.1.5 i nämnda förordning anges att gräns-, invandrings- och viseringsmyndigheter avses, vilket tydligt pekar ut en särskild krets av myndigheter i Sverige. Att även privata aktörer – utan att dessa begränsas på något sätt – omfattas av artikel 11.6 i id-kortsförordningen talar enligt vår mening mot att avsikten med att endast behöriga nationella myndigheter ska få genomföra en identitetskontroll mot en handling är att begränsa dessa utöver vad som eventuellt kan bestämmas av EU:s medlemsstater i nationell rätt. I förordningen anges inte heller att medlemsstaterna i en särskild ordning är skyldiga att utse eller ange vilka de behöriga nationella myndigheterna är vid tillämpningen av förordningen.

Mot denna bakgrund anser vi att id-kortsförordningen inte utgör någon begränsning av vilka myndigheter som bör kunna biometriskt verifiera identitet genom en kontroll mot handlingar, och än mindre mot ett identitetsindex.

[8] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008.

Myndighetsbegreppet

Samtliga statliga och kommunala organ, förutom riksdagen och de kommunala beslutande församlingarna (kommunfullmäktige och regionfullmäktige), är enligt regeringsformens terminologi myndigheter. Myndigheter är med andra ord de organ som ingår i den offentligrättsliga statliga och kommunala organisationen. Regeringen, domstolarna samt de statliga och kommunala förvaltningsmyndigheterna är alltså myndigheter.[9]

I tryckfrihetsförordningen tillämpas samma myndighetsbegrepp som i regeringsformen. Frågan om ett visst organ är en myndighet blir vid tillämpning av tryckfrihetsförordningen vanligtvis aktuell i samband med en begäran om att få tillgång till allmänna handlingar. Varken riksdagen eller region- och kommunfullmäktige utgör myndigheter i tryckfrihetsförordningens mening, men dessa beslutande församlingar jämställs uttryckligen med myndigheter i 2 kap. 5 §. Däremot är bolag, föreningar och stiftelser inte myndigheter ens om staten eller en kommun helt äger eller bestämmer över dem. Enligt 2 kap. 2 § offentlighets- och sekretesslagen – som motsvarar 2 kap. 5 § tryckfrihetsförordningen – ska riksdagen och beslutande kommunala församlingar jämställas med myndigheter vid tillämpningen av lagen. Vad som föreskrivs i tryckfrihetsförordningen om rätt att ta del av allmänna handlingar hos myndigheter ska, enligt 2 kap. 3 § offentlighets- och sekretesslagen, gälla även handlingar hos aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner och regioner utövar ett rättsligt bestämmande inflytande. Sådana bolag, föreningar och stiftelser ska vid tillämpningen av lagen jämställas med myndigheter. Det anges i bestämmelsens andra stycke när kommuner och regioner ska anses utöva ett rättsligt bestämmande inflytande. Vad som föreskrivs i tryckfrihetsförordningen om rätt att ta del av allmänna handlingar hos myndigheter ska i tillämpliga delar också gälla handlingar hos de organ som anges i bilagan till offentlighets- och sekretesslagen, om handlingarna hör till den verksamhet som nämns där. Detta framgår av 2 kap. 4 § offentlighets- och sekretesslagen. Dessa organ ska, vid tillämpningen av lagen, jämställas med myndigheter. I bilagan finns bland annat arbetslöshetskassorna vad gäller verksamheten med prövning av ärenden enligt lagen om arbets-

[9] Se 1 kap. 8 § regeringsformen och kommentaren till denna bestämmelse i *Grundlagarna, RF, SO och RO,* Holmberg, Stjernquist, Isberg, Eliason och Regner, JUNO Version 3 A, 2019-07-03.

löshetsförsäkring och av ärenden om medlemsavgift för arbetslös medlem.

Vi har ovan kommit fram till att statliga och kommunala myndigheter bör ha en möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar. Fråga är om andra aktörer – på liknande sätt som i tryckfrihetsförordningen och offentlighets- och sekretesslagen – bör jämställas med myndigheter vid användningen av ett sådant system för att säkert verifiera identitet. En grundläggande fråga i detta sammanhang är vilket behov av att kunna verifiera identitet biometriskt dessa aktörer kan anses ha.

Att riksdagen och region- och kommunfullmäktige jämställs med myndigheter vid tillämpningen av tryckfrihetsförordningen och offentlighets- och sekretesslagen grundar sig i det insynsintresse som finns för dessa aktörer. De kan däremot sällan antas komma i kontakt med personer vars identitet behöver verifieras och har, så vitt vi kan bedöma, därmed ett begränsat behov av att kunna biometriskt verifiera identitet mot ett index eller mot handlingar; till exempel får kommunfullmäktige vanligen ta del av det beslutsunderlag som en myndighet inom kommunen, till exempel en socialnämnd, har tagit fram. Ett eventuellt behov av biometrisk verifiering av identitet för kommunen kan därmed tillgodoses på annat sätt än genom att kommunfullmäktige genomför en sådan kontroll. Motsvarande får anses gälla för riksdag och regionfullmäktige. Riksdagen och beslutande kommunala församlingar bör enligt vår bedömning därmed inte jämställas med myndigheter vid tillämpning av ett system för att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

När det gäller statliga bolag, föreningar och stiftelser jämställs de inte med myndigheter vid tillämpningen av offentlighets- och sekretesslagen. Det gör däremot bolag, föreningar och stiftelser där kommuner och regioner utövar ett rättsligt bestämmande inflytande, enligt 2 kap. 3 § offentlighets- och sekretesslagen. Det handlar alltså om privaträttsliga subjekt. Även i det här avseendet är det insynsintresset i dessa aktörers verksamhet som motiverar att de jämställs med myndigheter.[10] Vi kan inte se att det är möjligt att inom ramen för denna utredning kartlägga och ta ställning till om det finns ett tydligt behov för dessa aktörer att kunna verifiera identitet biometriskt. Det finns därför enligt vår mening inte anledning att jämställa

[10] *Handlingsoffentlighet hos kommunala företag,* prop. 1993/94:48, s. 16 ff.

dem med myndigheter vid tillämpning av ett system för att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

De organ som anges i bilagan till offentlighets- och sekretesslagen är privaträttsliga subjekt. Det är vanligtvis fråga om organ som anförtrotts att fördela allmänna medel eller tilldelats andra myndighetsutövningsuppgifter, vilket är anledningen till att lagstiftaren har bedömt att de ska omfattas av handlingsoffentligheten, i den mån handlingar hos organet hör till den verksamhet som specificeras i bilagan.[11] Det är enligt vår mening inte lämpligt att, i ett regelverk avseende ett system för att biometriskt verifiera identitet mot antingen ett identitetsindex eller mot handlingar, ange att organen i bilagan till offentlighets- och sekretesslagen ska jämställas med myndigheter vid tillämpning av regelverket. Justeringar av organ och verksamheter i bilagan till offentlighets- och sekretesslagen skulle i sådant fall få direkt genomslag i det regelverk vi överväger. På samma sätt som gäller för ovan nämnda organ syftar bilagan till att upprätthålla offentlighetsprincipen och tillgodose insynsbehovet i vissa organs verksamhet. Vid justeringar i bilagan bör hänsyn inte behöva tas till annat än just insynsbehovet; eventuella konsekvenser vad gäller användningen av ett eventuellt system för att biometriskt verifiera identitet bör då inte behöva beaktas. Med hänsyn till dessa omständigheter anser vi att de organ som anges i bilagan till offentlighets- och sekretesslagen inte bör jämställas med myndigheter vid tillämpning av ett system för att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

Kretsen av myndigheter bör inte initialt inskränkas

I detta sammanhang kan det övervägas om det finns skäl att på något sätt särskilt avgränsa den krets av myndigheter som vi ovan bedömt bör få möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar. Det finns ett stort antal myndigheter i Sverige och alla har inte samma faktiska behov av att kunna genomföra en biometrisk verifiering av identitet i sin verksamhet. Detta kan särskilt antas gälla för myndigheter som handlägger få ärenden som rör enskilda. Exempelvis kan myndigheter som Riksrevisionen, Kemikalieinspektionen och Medlingsinstitutet sällan antas behöva verifiera

[11] Regeringens prop. 1986/87:151 *om ändringar i tryckfrihetsförordningen m.m.*, s. 148 ff.

identitet för enskilda personer. Det bör dock understrykas att detta endast är ett antagande om ett generellt behov, vilket inte behöver utesluta att även nämnda myndigheter i det enskilda fallet kan ha ett behov av att kunna biometriskt verifiera identitet för en person som man möter inom ramen för handläggningen av ett visst ärende eller i något annat sammanhang. I betänkandet *Ett säkert statligt ID-kort – med e-legitimation* anfördes, i samband med överväganden om krav på identifiering med statliga fysiska identitetshandlingar skulle föreslås på olika områden, bland annat följande.

> Att införa krav på identifiering genom uppvisande av en statlig fysisk identitetshandling på områden där det inte i dag finns någon reglering om hur identitetskontrollen ska gå till skulle dessutom innebära att konsekvenserna på varje område behöver övervägas mer noggrant än vad det finns utrymme till inom ramen för denna utredning. Det rör sig om vitt skilda områden vilket innebär att olika överväganden behöver göras för varje område.[12]

En möjlighet för myndigheter att biometriskt verifiera identitet mot ett index eller mot handlingar kan kräva samma typ av överväganden, vilket talar för att på något sätt, åtminstone initialt, begränsa kretsen av myndigheter som bör kunna omfattas av en sådan eventuell möjlighet. Att verifiering av identitet med hjälp av biometriska uppgifter innebär behandling av känsliga personuppgifter och medför ett visst intrång i den personliga integriteten (se avsnitt 21.7.2) talar i samma riktning. Samtidigt kan vi konstatera att vårt uppdrag uttryckligen tar sikte på att lämna förslag som breddar möjligheterna till säkrare verifiering av identitet, med hjälp av biometriska uppgifter. Utgångspunkten bör därför vara att ingen inskränkning bör göras. Det är enligt vår mening inte heller möjligt att inom ramen för denna utredning ta ställning till de faktiska behoven och förutsättningarna för samtliga myndigheter och lämna förslag som pekar ut vissa särskilt angivna myndigheter, utan att en sådan uppräkning riskerar att framstå som godtycklig. Det skulle också kunna uppfattas som att en säker kontroll av identitet inte bör tillämpas eller prioriteras hos de myndigheter som *inte* pekas ut.

Ett alternativ skulle kunna vara att ge regeringen bemyndigande att i förordning – efter nödvändiga överväganden avseende den enskilda myndighetens behov och förutsättningar att genomföra identitetskontroller – närmare peka ut vilka myndigheter som bör få möj-

[12] SOU 2019:14, s. 195.

lighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar. På detta sätt skulle ”behöriga” myndigheter pekas ut, vilket också ligger i linje med den begreppsapparat som används i bland annat EU:s id-kortsförordning. En ordning som innebär att kretsen av myndigheter måste utökas efterhand har emellertid den nackdelen att det kan komma att dröja innan myndigheter med ett konkret behov faktiskt kan utnyttja en utökad möjlighet till biometrisk verifiering av identitet. Det framstår vidare som lämpligt att frågan om hur en viss myndighet bör hantera identitetskontroller inom ramen för sin specifika verksamhet hanteras och regleras på myndighetsnivå, genom myndighetsinterna föreskrifter eller riktlinjer, som är utformade på ett för verksamheten ändamålsenligt sätt; i 2017 års ID-kortsutredning anfördes – i fråga om de myndigheter som betalar ut olika förmåner från välfärdssystemen – att i de sammanhang en riktig identitetskontroll behöver göras av dem ”utgår vi från att dessa kommer att införa rutiner som stämmer överens med de förslag vi lämnar och de bedömningar vi gör”.[13] Motsvarande kan enligt vår mening antas gälla inom ramen för detta betänkande. Vi anser att det mot denna bakgrund kan ifrågasättas om det, av annan anledning än en ökad tydlighet och förutsebarhet, är nödvändigt eller lämpligt att initialt inskränka vilka myndigheter som bör kunna få biometriskt verifiera identitet mot ett index eller mot handlingar. Tillräcklig tydlighet och förutsebarhet kan i stället uppnås genom att myndigheter tar fram nödvändiga, interna, riktlinjer för när biometrisk verifiering bör eller ska användas i myndighetens verksamhet. Det är även möjligt för berörda myndigheter att informera om att biometriska identitetskontroller kan komma att användas i verksamheten, exempelvis genom att detta framgår av myndighetens hemsida eller informationsmaterial som den enskilde kan ta del av i samband med att ett ärende inleds; redan i dag informerar exempelvis Försäkringskassan på sin hemsida om hur en ansökan om olika förmåner går till.[14]

Vid en sammantagen bedömning av det ovan anförda anser vi att kretsen av myndigheter inte bör begränsas.

[13] SOU 2019:14, s. 194.
[14] Se https://www.forsakringskassan.se/privatperson/studerande/bostadsbidrag-till-unga-under-29-ar, senast besökt den 8 juli 2026.

21.3.2 Privata aktörer

Vår bedömning

Privata aktörer bör, i nuläget, inte omfattas av en ny lag som reglerar en generell möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

Vi ska, enligt vårt uppdrag, utvärdera om såväl statliga myndigheter som andra offentliga aktörer och privata aktörer bör omfattas av en möjlighet att använda biometriska uppgifter för en stärkt verifiering av identitet i olika sammanhang. Frågan är därmed om även privata aktörer, exempelvis företag, bör omfattas av en eventuell ny lag som reglerar en generell möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar, i likhet med vad vi kommit fram till avseende myndigheter i föregående avsnitt. Frågan om privata aktörers tillgång till och användning av biometriska uppgifter är som vi ser det nära förknippad med grundläggande rättsstatliga principer, EU-rättsliga och konventionsgrundade krav på skydd för personuppgifter samt nationella krav på rättssäkerhet. Det finns – på de skäl vi redogör för nedan – flera rättsliga och principiella hinder mot att ge privata aktörer en möjlighet att med stöd av lag biometriskt verifiera identitet mot såväl ett identitetsindex som mot handlingar.

Privata aktörers behov varierar betydligt

Av stor betydelse för den aktuella bedömningen är enligt vår mening att det kan konstateras att det finns ett tydligt behov av att kunna genomföra biometriska verifieringar av identitet. Det kan visserligen antas att även privata aktörer har ett behov av att kunna säkerställa att den person man möter är den som han eller hon utger sig för att vara. Kontroll av identitet kan utgöra ett betydelsefullt led i att motverka identitetsmissbruk som kan förekomma vid exempelvis ett köp, eller vid leverans av en vara. För det fall privata aktörer ges ett stöd i lag för att använda biometrisk verifiering mot ett index eller mot handlingar bör det dock vara förbehållet de aktörer som har ett mycket tydligt behov av att verifiera identitet, utifrån arten på den bedrivna verksamheten. Detta med hänsyn till i första hand det ingrepp i den personliga integriteten som biometrisk verifiering innebär (se av-

snitt 21.7). Vidare behöver en möjlighet till biometrisk verifiering mot handlingar – som vi redogjort för i avsnitt 21.2 – regleras i lag, och en förutsättning för sådan verifiering är att myndigheten har möjlighet att begära att den enskilde gör handlingen tillgänglig för kontroll. Detsamma gäller om en privat aktör ska få ställa ett sådant krav. Vi kan visserligen inte se något direkt rättsligt hinder mot att ge privata aktörer möjlighet att begära att den enskilde gör en handling tillgänglig för biometrisk verifiering. Ett sådant mandat medför dock en utökad maktställning i förhållande till den person vars identitet behöver kontrolleras, och innebär att den enskilde dels behöver göra en handling tillgänglig, dels behöver lämna biometriska underlag till den privata aktören som kan användas för kontrollen.

För myndigheter står det enligt vår mening klart att det finns ett tydligt behov av att kunna biometriskt verifiera identitet framför allt i samband med handläggningen av ett ärende, redan med hänsyn till att en myndighet alltid måste veta vem som är part i ärendet, för att en korrekt bedömning ska kunna göras och för att ett beslut ska kunna fattas avseende rätt person. Identitetsmissbruk kan dock även få stora konsekvenser för privata aktörer, exempelvis vid kreditbedrägerier, som förekommer i stor utsträckning i Sverige. Kostnader som kan uppstå vid identitetsbedrägerier inkluderar direkta ekonomiska förluster från lån och varor samt direkta kostnader för att reda ut situationen, exempelvis i form av advokatkostnader eller kostnader för att få nya identitetshandlingar utfärdade. Av statistik från Brottsförebyggande rådet framgår att antalet anmälda identitetsbedrägerier visserligen har minskat kraftigt under senare år, från 27 901 år 2020 till 9 872 år 2024.[15] Behovet av att kunna verifiera identitet på ett tillförlitligt sätt är enligt vår mening dock fortsatt aktuellt, inte minst med hänsyn till de stora kostnader som bedrägerierna för med sig; av statistik framgår att brottsvinsterna bara från identitetsbedrägerier uppskattades till 516 miljoner kr år 2024. När det gäller behov av verifiering av identitet av framgår av svar från en privat aktör på den enkätundersökning som vi genomfört (se avsnitt 2.3) bland annat följande.

[15] Statistik över anmälda brott, hämtat från BRÅ:s hemsida.

> För medborgare medför ökad användning av biometri för att kontrollera identiteten att processer blir enklare, säkrare och mer tillgängliga. För bankerna medför ökad användning av biometri att utvecklingen av digitala banktjänster för både konsumenter och företag blir mer säkra och mer tillgängliga.

Verifiering med hjälp av biometriska uppgifter skulle, som vi ser det, kunna vara ett effektivt sätt för många enskilda aktörer att motverka bedrägerier av olika slag där identitetsmissbruk är ett centralt moment. Genom att ge privata aktörer ett stöd i lag för att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar skulle dessa kunna skyddas mot ekonomiska förluster förknippade med bedrägerier, men även privatpersoner kan på detta sätt ges ett bättre skydd mot id-kapning. Att det för privata aktörer som kollektiv skulle finnas ett tydligt behov av att kunna använda biometrisk verifiering, och att en sådan möjlighet endast skulle föra med sig positiva effekter, är dock inte entydigt. I den enkätundersökning som vi genomfört anförde exempelvis en aktör inom försäkringsbranschen att man inte alls ser några positiva konsekvenser av en möjlighet att ta upp biometri, varken i den egna organisationen eller i försäkringsbranschen i stort, och att nuvarande ordning där en försäkringstagares identitet kontrolleras i samband med ingående av försäkringsavtal – genom att personnummer anges och BankID används för autentisering – är ett fullgott verktyg. Man lyfte även fram att användning av biometri skulle leda till stora kostnader och komplicera handläggning och distribution av produkter på ett sätt som varken är nödvändigt eller motiverat. I slutändan skulle ett sådant system, enligt enkätsvaret, riskera att leda till högre premier för försäkringstagarkollektivet. Dessa faktorer kan, enligt vår mening, inte bortses från och gör sig – i vart fall i fråga om kostnader för enskilda personer – inte gällande på samma sätt för myndigheter.

Även med beaktande av det ovan anförda bedömer vi att en stärkt möjlighet för privata aktörer att biometriskt verifiera identitet skulle kunna främja ett skydd mot ekonomiska förluster förknippade med bedrägerier. Privatpersoner skulle på detta sätt ges ett bättre skydd mot id-kapning. Det kan också påpekas att det skulle vara fråga om just en möjlighet – och inte en skyldighet – för privata aktörer att biometriskt verifiera identitet vid behov. Samtidigt är det enligt vår mening svårt att närmare konkretisera vilka behov privata aktörer har, då detta kollektiv är många gånger större än antalet myndigheter,

och bedriver verksamhet av synnerligen varierande slag. Antalet myndigheter är förvisso också stort, men går som vi ser det inte att jämföra med antalet privata aktörer i samhället. Även om det faktiska behovet kan antas variera mellan myndigheter har de en betydande möjlighet att genom egna föreskrifter och myndighetsinterna riktlinjer på ett enhetligt sätt identifiera behov av stärkt identitetskontroll och anpassa verksamheten utifrån dessa behov. Lagstiftaren och regeringen har också en möjlighet att genom författning, regleringsbrev och andra styrdokument påverka myndigheternas arbete med att motverka identitetsmissbruk som riktar sig mot samhället. En motsvarande styrning är som vi ser det inte möjlig att implementera eller upprätthålla för privata aktörer. Arbetet mot identitetsmissbruk kan på nämnda sätt bedrivas på ett sammanhållet sätt av det offentliga även om enskilda myndigheters behov kan variera, och det kan därför anses finnas ett gemensamt behov på ett annat sätt än hos privata aktörer. Behovet är i fråga om myndigheter, enligt vår mening, också tydligare knutet till ett allmänt intresse av att motverka identitetsmissbruk än vad som är fallet för privata aktörer, vars verksamhet många gånger i första hand drivs av ekonomiska intressen.

Att öppna upp en möjlighet för samtliga privata aktörer att med stöd av en ny lag biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar riskerar alltså att vila på ett otydligt behov som endast föreligger för en liten del av detta kollektiv. En generell rätt för privata aktörer att biometriskt verifiera identitet riskerar som vi ser det att leda till att sådan verifiering genomförs även i situationer då integritetsintrånget inte är motiverat utifrån den privata aktörens behov, antingen allmänt sett utifrån bedriven verksamhet eller i det enskilda fallet, till exempel för att det handlar om en transaktion av begränsat ekonomiskt värde. Det är enligt vår mening inte heller lämpligt att här peka ut endast vissa branscher eller sektorer; detta skulle kräva överväganden som inte ryms inom vårt uppdrag eller den tidsram vi har till vårt förfogande, och skulle även kunna framstå som godtyckligt, oavsett hur gränsdragningen görs.

Krav på tydlighet och förutsebarhet är svåra att upprätthålla

Det övergripande ändamålet med den behandling av personuppgifter som behöver utföras vid biometrisk verifiering av identitet mot ett identitetsindex eller mot handlingar är att motverka identitetsmissbruk. Regeringen har i propositionen *Anpassning av svensk rätt till den reviderade VIS-förordningen* bedömt att motverkandet av identitetsbedrägerier utgör ett viktigt allmänt intresse.[16] Vi delar denna bedömning (se avsnitt 16.4.3). Även med denna utgångspunkt skulle det enligt vår mening krävas någon form av begränsning av i vilka situationer en privat aktör bör få använda biometrisk verifiering med stöd av lag mot ett index eller mot handlingar; en helt oreglerad möjlighet att använda sådana kontroller skulle enligt vår bedömning inte vara proportionerlig.

När det gäller biometrisk verifiering av identitet mot handlingar krävs, som vi redogjort för i avsnitt 21.2, i vart fall för de handlingar som omfattas av de EU-förordningar som vi redogjort för i avsnittet, stöd i nationell lagstiftning för att myndigheter ska få kräva att handlingen och därmed de biometriska underlag som är lagrade i den görs tillgängliga för kontroll. Detsamma gäller för privata aktörer. Sådant stöd i lag behöver vara utformat på ett sätt som innebär att tillämpningen blir tydlig och förutsebar. Ett krav på stöd i lag, som är tydligt utformat, gäller även den behandling av personuppgifter – däribland känsliga sådana – som behöver utföras vid en biometrisk verifiering mot en handling. EU-domstolen har i fråga om handlingar som omfattas av EU:s id-kortsförordning uttalat att den uppgiftsbehandlingen är av sådant slag att den kan ge ytterligare information om de berörda personernas privatliv och att den därför endast får ske för ändamål som är strikt begränsade till att identifiera den berörda personen och under vissa klart avgränsade förutsättningar i den lag som innehåller kravet på uppvisande av identitetskort eller uppehållshandling (se EU-domstolens dom i mål C-61/22, *Landeshauptstadt Wiesbaden*, punkt 116).

Frågan är hur krav på tydlighet och förutsebarhet kan upprätthållas för privata aktörer. En avgränsning som utgår från handläggningen av ett ärende är av naturliga skäl inte möjlig att göra för privata aktörer, på det sätt som kan göras för myndigheter (se avsnitt 21.5.1). Det är enligt vår mening inte heller lämpligt att avseende privata

[16] Prop. 2024/25:176, s. 39.

aktörer knyta användningen till att en identitetskontroll genomförs i annat fall, på det sätt vi redogör för i avsnitt 21.5.2. Detta med hänsyn till att privata aktörers verksamhet inte är reglerad på samma sätt som för myndigheter, dels genom allmänna förvaltningsrättsliga författningar – exempelvis 5 § förvaltningslagen (2017:900) som anger att en myndighet endast får vidta åtgärder som har stöd i rättsordningen – dels genom eventuella sektorspecifika regelverk som anger vilken typ av verksamhet som en myndighet ska och får bedriva, exempelvis i form av myndighetsinstruktioner. Dessa regelverk främjar en tydlighet och förutsebarhet, som saknas på motsvarande sätt för privata aktörer. En möjlighet att använda biometrisk verifiering av identitet, som är knuten till att den får genomföras i samband med att en identitetskontroll genomförs i annat fall än vid handläggningen av ett ärende, innehåller visserligen ett bedömningsutrymme för myndigheten. Det är dock begränsat dels av ovan nämnda skäl, dels av allmänna krav på myndigheter i fråga om saklighet och objektivitet. För privata aktörer bedömer vi däremot att bedömningsutrymmet skulle vara alltför stort, vilket skulle betydligt öka risken för sådan ändamålsglidning som vi återkommer till nedan, och de särskilda risker som detta i sin tur för med sig.

Det skulle i stället kunna övervägas att knyta privata aktörers användning till situationer då identitetsbedrägerier aktualiseras, i första hand de som är hänförliga till lån, köp och kreditgivning. En gemensam nämnare för dessa former av bedrägerier är att de bygger på ingående eller fullgörande av någon form av avtal i något led, exempelvis vid ett köp av en vara på distans. Att knyta privata aktörers möjlighet att biometriskt verifiera identitet till situationer som innebär att ett avtal ingås eller fullgörs skulle därför kunna vara ett alternativ. Det finns emellertid inte samma naturliga samband mellan identitetens betydelse och ingåendet eller fullgörandet av ett avtal som det finns i vart fall vid handläggningen av ett ärende enligt förvaltningslagen; enligt 19 § förvaltningslagen framgår uttryckligen att identitetsuppgifter ska lämnas när någon inleder ett ärende hos en myndighet. Vi kan vidare konstatera att vad som utgör ett avtal i det enskilda fallet får avgöras utifrån civilrättsliga regler, vilket kan kräva tolkning av parterna. Vad som utgör ett ärende hos en myndighet, och vem som är part i ärendet, torde däremot sällan medföra några svårigheter att avgöra. Det framstår inte heller som proportionerligt att privata

aktörer ges möjlighet att biometriskt verifiera identitet i samtliga avtalssituationer.

Det är visserligen rimligt att utgå från att en privat aktör i normalfallet inte kommer att besvära sig om att genomföra en biometrisk verifiering vid ingående eller fullgörande av ett avtal av begränsat ekonomiskt värde. För att det integritetsintrång en biometrisk verifiering innebär ska vara motiverat med hänsyn till den privata aktörens behov skulle det emellertid, som vi ser det, förutsättas att ytterligare rekvisit är uppfyllda för att en verifiering ska vara tillåten, exempelvis att avtalet motsvarar ett visst värde eller att det finns omständigheter som talar för att det är fråga om ett bedrägeriförsök. Sådana, eller liknande, villkor skulle kräva ytterligare bedömningar och riskera att skapa ytterligare otydlighet och oförutsägbarhet. Varken de privata aktörerna eller de personer vars identitet behöver verifieras skulle med enkelhet kunna avgöra om de rättsliga förutsättningarna för en sådan kontroll är uppfyllda eller inte.

Det har enligt vår mening inte i övrigt kommit fram något lämpligt sätt att på ett tydligt och förutsebart sätt reglera under vilka förutsättningar privata aktörer bör få möjlighet att verifiera identitet mot ett index eller mot handlingar. Som vi konstaterat ovan varierar dessa aktörers behov stort och vi är tveksamma till att det på ett enhetligt och överskådligt sätt går att i författning specificera när de i så fall bör få verifiera identitet biometriskt. En träffsäker reglering – som endast möjliggör verifiering när det är proportionerligt – riskerar att bli mycket detaljerad och svårtillämpad.

Risker för bristande förenlighet med dataskyddsförordningen

Biometrisk verifiering av identitet mot ett index eller mot handlingar innebär att olika personuppgifter, däribland känsliga sådana, behöver behandlas. För det fall privata aktörer skulle ges stöd i en ny lag för att genomföra sådana kontroller ankommer det på aktören i fråga att säkerställa att behandlingen i ett visst fall är tillåten, det vill säga att personuppgifterna behandlas på ett lagligt, korrekt och öppet sätt (se artikel 5.1 a och 5.2 i dataskyddsförordningen[17]). Med hänsyn till privata aktörers kraftigt skiftande verksamheter och behov av biomet-

[17] 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).

risk verifiering är det inte möjligt för lagstiftaren att på ett generellt sätt ta ställning till om det för dessa finns en tillämplig rättslig grund för behandlingen eller göra de proportionalitetsavvägningar som är nödvändiga. Att inte på förhand kunna ta ställning till om en privat aktör som vill verifiera identitet biometriskt har en rättslig grund för detta – och i så fall vilken – innebär enligt vår mening en risk för att behandlingen inte kommer att vara förenlig med grundläggande principer i dataskyddsförordningen, däribland den princip om ändamålsbegränsning som anges i artikel 5.1 b.

Risken för så kallad ändamålsglidning – det vill säga att uppgifter efter insamlingen används för nya eller utökade syften – måste enligt vår mening också särskilt beaktas avseende privata aktörer, mot bakgrund av att det ankommer på aktören i fråga att se till att behandlingen av personuppgifter är laglig och att den utförs korrekt. Privata aktörer verkar i en annan ekonomisk kontext än myndigheter, och data betraktas inte sällan som en strategisk resurs. Ett tydligt allmänt intresse som grund för personuppgiftsbehandlingen kan ofta saknas. Det kan därför finnas ett incitament för privata aktörer att maximera värdet av investeringar som gjorts i ett insamlings- och verifieringssystem, att återanvända uppgifter för nya affärsmässiga ändamål eller att kombinera uppgifterna med andra datakällor. Även om den ursprungliga, tillåtna användningen skulle vara tillräckligt snävt definierad i lag, till exempel genom att den begränsas till avtalssituationer, kan det finnas ett incitament hos en privat aktör att bredda användningen, exempelvis till användarprofilering eller risk- och kreditbedömning. En sådan utveckling kan ske gradvis utan tydliga beslutspunkter, vilket försvårar rättslig kontroll. En avtalsrättslig legitimering av ändamålen riskerar att urholka ändamålsbegränsningsprincipen i praktiken eftersom en användare sällan har reell möjlighet att motsätta sig avtalsändringar, vilket i sin tur innebär en risk för ytterligare maktobalans och därmed ett bristande samtycke i dataskyddsförordningens mening.

Risken för ändamålsglidning är enligt vår mening betydligt större avseende privata aktörer än för myndigheter, bland annat genom att det inte finns motsvarande rättsliga eller institutionella kontrollmekanismer för de förstnämnda. Myndigheter är bundna av legalitetsprincipen, vilket innebär att all behandling av personuppgifter måste ha stöd i lag och ligga inom ett klart definierat verksamhetsområde. En privat aktör kan i stället använda interna affärsbeslut för att efter hand utvidga sin verksamhet. De rättsliga spärrarna är därmed mindre ro-

busta än i offentlig sektor. Myndigheter omfattas vidare av tillsyn genom Riksdagens ombudsmän (JO), av objektivitets- och proportionalitetsprinciper samt av krav på offentlighet och transparens på ett annat sätt än privata aktörer. Beslut av en myndighet kan också normalt angripas med stöd av bestämmelser om överklagande till allmän förvaltningsdomstol. Privata aktörer står visserligen under tillsyn av Integritetsskyddsmyndigheten vid behandling av personuppgifter, men omfattas inte av samma krav på insyn, motiveringsskyldighet i samband med att beslut fattas, eller förutsebarhet, som gäller för myndigheter. Sammantaget skapar detta, som vi ser det, en reaktiv snarare än proaktiv kontrollmiljö, där en ändamålsglidning kan etableras innan en eventuell rättslig prövning sker. Enskilda som hos en privat aktör kan bli föremål för en biometrisk verifiering har därmed svagare rättsmedel att ta till vid felaktig behandling eller missbruk.

Till detta kommer att om privata aktörer skulle ges ett generellt stöd i lag för att använda biometrisk verifiering mot ett index eller mot handlingar saknas det hinder mot att de själva implementerar de tekniska lösningar som krävs för att utföra sådana kontroller i sin verksamhet. Biometriska system är ofta tekniskt generella; samma biometriska underlag och uppgifter kan användas i flera olika applikationer. Detta innebär att den tekniska tröskeln för vidarebehandling är relativt låg och att nya användningsområden kan införas utan att biometriska underlag samlas in på nytt. Det kan vara svårt – både från samhällets och enskildas sida – att kontrollera att en begränsning av hur biometriska uppgifter får behandlas efter kontrollen efterlevs. För privata aktörer där verksamheten i sig, och de ändamål som personuppgifter får behandlas för, normalt inte är reglerade i lag eller annan författning på samma sätt som för myndigheter – exempelvis genom myndighetsinstruktioner och särskild registerlagstiftning – innebär detta en ytterligare ökad risk för ändamålsglidning.

En annan risk – utifrån att den privata aktören skulle ha att bedöma om det finns en rättslig grund – är att det får betydelse *vem,* hos exempelvis ett företag, som genomför en biometrisk verifiering i det enskilda fallet. Vi kan notera att det av EU:s id-kortsförordning framgår att endast vederbörligen bemyndigad personal ska få använda biometriska uppgifter i handlingar för att kontrollera identitet (artikel 11.6). Detta gäller både för myndigheter och för privata aktörer. Myndigheter har emellertid myndighetsspecifika föreskrifter, riktlinjer och arbetsindelningar. Den som utövar myndighet kan också

ådra sig straffrättsliga konsekvenser genom regler om tjänstefel. På detta sätt kan myndigheter i tillräcklig grad säkerställa att endast personal med nödvändig kompetens och behörighet är bemyndigad att utföra olika arbetsuppgifter. Motsvarande institutionell och rättslig kontroll saknas, som vi ser det, hos privata aktörer. Även detta ökar risken för att behandlingen av personuppgifter – i samband med biometrisk verifiering av identitet mot ett identitetsindex eller mot handlingar – inte skulle stå i överensstämmelse med dataskyddsförordningen.

Risker för den personliga integriteten

För att biometrisk verifiering av identitet mot ett identitetsindex eller mot handlingar ska kunna genomföras förutsätts att en ansiktsbild och/eller fingeravtryck tas. Att ta en ansiktsbild utan en persons samtycke kan under vissa omständigheter anses utgöra ett intrång i privatlivet i den mening som avses i artikel 8 i Europakonventionen och artikel 7 och 8 i EU:s rättighetsstadga.[18] Samtidigt ska beaktas att själva upptagningen av en ansiktsbild inte innebär något ingrepp i intimsfären och inte heller medför något större fysiskt eller psykiskt obehag för personen (EU-domstolens mål C-70/18, *Staatsecretaris van Justitie en Veiligheid mot A m.fl.*, punkt 58). Att ta någons fingeravtryck är däremot ett sådant kroppsligt ingrepp som omfattas av skyddet i 2 kap. 6 § första stycket regeringsformen. Även framtagning av biometriska uppgifter ur ansiktsbilden och fingeravtryck, och jämförelsen mot de uppgifter som finns lagrade i den handling som används för verifieringen, medför ett visst intrång i den personliga integriteten, och det skydd för denna som framgår av bland annat artikel 8 i Europakonventionen (se avsnitt 21.7.3). En möjlighet för privata aktörer att ta upp en ansiktsbild eller fingeravtryck innebär som vi ser det särskilda risker för den personliga integriteten, genom att den enskilde behöver lämna biometriska underlag till en privat aktör utan offentlig kontroll. Den privata aktören skulle – vid biometrisk verifiering av identitet mot handlingar – även behöva behandla känsliga personuppgifter. Vid verifiering mot ett identitetsindex skulle de biometriska uppgifterna, enligt vår bedömning, i stället tas fram av systemet, inte av den aktör som tar upp biometriska underlag (se

[18] *Biometri i brottsbekämpningen*, prop. 2024/25:37, s. 47.

avsnitt 18.3.3). När det gäller biometrisk verifiering av identitet mot handlingar kan vi notera att 2017 års ID-kortsutredning ansåg att sådana kontroller åtminstone vid den tidpunkten inte skulle tillåtas.[19]

Europadomstolen har klargjort att artikel 8 i Europakonventionen inte endast innebär att staterna är skyldiga att avstå från alla åtgärder som kan innebära att rätten överträds, utan staten har under vissa omständigheter även en positiv skyldighet att aktivt säkerställa effektiv respekt för privat- och familjeliv.[20] De faktorer som vi lyft fram ovan i fråga om en risk för ändamålsglidning medför som vi ser det också indirekt en risk för framtida, oförutsedda användningar av biometriska underlag av privata aktörer och att enskilda personer exponeras för integritetsintrång. Om privata aktörer implementerar egna tekniska lösningar och sparar biometriska underlag i strid med ett regelverk för ett generellt system för biometrisk verifiering av identitet, ökar riskerna för dataintrång och missbruk. Eftersom det är fråga om behandling av biometriska underlag och biometriska uppgifter är eventuella skador för den enskilde irreversibla, till skillnad från lösenord eller identitetshandlingar som kan bytas ut. Detta ställer högre krav på proportionalitetsbedömningen och talar enligt vår mening starkt för att endast aktörer med särskilda rättsliga och organisatoriska garantier och kontrollmekanismer – i vår mening myndigheter – bör omfattas av en eventuell ny lag som reglerar en generell möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

Vi anser mot denna bakgrund att det skulle medföra betydande svårigheter för staten att uppfylla de positiva skyldigheter som följer av artikel 8 i Europakonventionen vid en möjlighet för privata aktörer att med stöd av en ny lag biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar. I förhållande till privata aktörer skulle, som vi nämnt ovan, den enskildes rättsmedel också vara mer begränsade vid en behandling som inte är proportionerlig och som därmed potentiellt sett står i strid med skyddet för den personliga integriteten i Europakonventionen och EU:s rättighetsstadga.

[19] SOU 2019:14, s. 312.
[20] Se exempelvis *Söderman mot Sverige*, nr 5786/08, *I. mot Finland*, nr 20511/03 och *K.U. mot Finland*, nr 2872/02.

Sammanfattande bedömning

En möjlighet att använda biometriska uppgifter för att verifiera identitet är enligt gällande rätt förbehållen en mycket begränsad krets av myndigheter, i vissa särskilt angivna ärendeslag och situationer. En reform i enlighet med våra bedömningar i avsnitt 21.5 skulle därmed i sig utgöra en betydande utvidgning av sådana typer av kontroller i samhället. Vidare skulle ett system med ett identitetsindex vara en helt ny företeelse i svensk identitetsförvaltning. Ett regelverk som ger myndigheter möjlighet att biometriskt verifiera identitet mot ett sådant index skulle därmed innebära dels ett nytt säkrare sätt att verifiera identitet biometriskt, dels att fler offentliga aktörer får möjlighet att verifiera identitet biometriskt i förhållande till vad som gäller i dag och de förslag som bereds i Regeringskansliet. Det finns enligt vår mening anledning att utvärdera utfallet av utvidgningar av angivna slag innan ett generellt stöd i lag för biometriska kontroller mot ett index eller mot handlingar eventuellt utökas till att även avse privata aktörer.

Under alla omständigheter anser vi att en möjlighet för privata aktörer att verifiera identitet mot ett identitetsindex eller mot handlingar måste motiveras av ett tydligt behov och det måste finnas ett tydligt och förutsebart lagstöd för att vidta en åtgärd som innebär att biometriska underlag tas upp och biometriska uppgifter behandlas. Det måste även säkerställas att behandlingen är förenlig med dataskyddsförordningen och skyddet för den personliga integriteten. Utifrån de omständigheter vi redogjort för ovan anser vi att det är mycket tveksamt om det går att säkerställa att dessa krav uppnås. Det finns, som vi ser det, en alltför stor risk att en möjlighet för privata aktörer att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar inte är förenlig med vare sig dataskyddsförordningen eller skyddet för den personliga integriteten enligt regeringsformen, Europakonventionen eller EU:s rättighetsstadga. Mot denna bakgrund anser vi att privata aktörer, i nuläget, inte bör omfattas av en ny lag som reglerar en generell möjlighet att biometriskt verifiera identitet mot ett identitetsindex eller mot handlingar.

Det skulle kunna övervägas att, genom ett bemyndigande i lag, ge regeringen en rätt att i förordning reglera privata aktörers möjlighet att använda biometrisk verifiering mot ett identitetsindex eller mot handlingar. Eftersom en möjlighet till biometrisk verifiering behöver regleras i lag skulle det inte vara möjligt för regeringen att besluta om

detta med stöd av den så kallade restkompetensen (jfr avsnitt 23.9). Ett särskilt bemyndigande för regeringen skulle dock göra det möjligt för regeringen att på förordningsnivå – utifrån att ett tydligt behov kan identifieras och efter noggranna överväganden avseende sådana faktorer som vi lyft fram ovan – utöka kretsen av aktörer som skulle få använda biometrisk verifiering av identitet. Exempelvis skulle det kunna vara fråga om aktörer vars verksamhet omfattas av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism. Som vi redogjort för ovan anser vi emellertid att det finns anledning att utvärdera utfallet av ett generellt stöd i lag för biometriska kontroller mot ett index eller mot handlingar för myndigheter, innan detta eventuellt utökas till att även avse privata aktörer. Ett bemyndigande i lag skulle innebära ett betydande utrymme för regeringen att i förordning bredda tillämpningsområdet på sätt som inte går att i tillräcklig grad förutse. Bland annat bedömer vi att det för privata aktörer är betydligt svårare att definiera i vilka situationer biometrisk verifiering skulle få användas, i vart fall om möjligheten ska träffa annat än en mycket smal krets, vilket i och för sig skulle kunna vara relevant. Med hänsyn till att det är fråga om ingrepp i den personliga integriteten som kan påverka en mycket stor grupp av personer – inklusive barn – och att biometrisk verifiering förutsätter behandling av känsliga personuppgifter, anser vi också att mycket stor försiktighet är påkallad vad gäller att införa bestämmelser som möjliggör biometrisk verifiering i annat än lag.

Mot denna bakgrund avser vi inte att lämna några förslag som innebär att regeringen får ett särskilt bemyndigande att i förordning föreskriva att även privata aktörer ska få möjlighet att verifiera identitet biometriskt.

21.4 Brottsbekämpande verksamhet

Vår bedömning

En generell möjlighet för myndigheter att i brottsbekämpande verksamhet verifiera identitet biometriskt – mot ett identitetsindex eller mot en handling – bör utredas i annan ordning.

Vi har i avsnitt 18.2.1 bedömt att *identifiering* av en person i ett identitetsindex bör vara tillåten endast för att kunna avgöra om en identitetsnyckel ska skapas. Ett index bör, enligt vår mening, alltså inte kunna användas för identifiering i andra situationer och därmed inte i den brottsbekämpande verksamheten. Vidare är det inte möjligt att identifiera en person genom att kontrollera biometriska uppgifter som kan tas fram ur biometriska underlag i en handling som han eller hon innehar. Frågan som kvarstår är därmed om det, inom ramen för vårt uppdrag, bör utvärderas om en myndighet bör kunna *verifiera* identitet biometriskt – mot ett identitetsindex eller mot en handling – i brottsbekämpande verksamhet.

Med *brottsbekämpande verksamhet* avses i vid bemärkelse sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Brottsdatalagen (2018:1177) gäller även vid personuppgiftsbehandling som en brottsbekämpande myndighet utför i syfte att upprätthålla allmän ordning och säkerhet. I lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna har brottsbekämpande verksamhet definierats som sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott (3 §). Vi återkommer i avsnitt 23.4 till den närmare innebörd begreppet brottsbekämpande verksamhet bör ha vid tillämpning av det regelverk vi föreslår.

Den centrala regleringen av villkoren för den brottsutredande verksamheten finns i rättegångsbalken och i författningar som ansluter till balken. Regleringen innehåller bland annat detaljerade bestämmelser om vilka åtgärder som ska vidtas under förundersökningens olika skeden och om vilka processuella krav som gäller för användningen av straffprocessuella tvångsmedel. Regleringen innebär sammantaget att förutsättningarna och förfarandet för den brottsutredande verksamheten regleras på ett förhållandevis ingående sätt. Reglerna har tillkommit som ett resultat av en noggrann avvägning mellan intresset av att säkerställa enskildas berättigade krav på rättssäkerhet å ena sidan och intresset av att brott utreds på ett snabbt och effektivt sätt å andra sidan. När det gäller den brottsförebyggande verksamheten är regleringen mer begränsad till sin omfattning. Inom ramen

för den brottsförebyggande verksamheten ryms vidare sådan verksamhet som utgör olika former av förstadier till en förundersökning.[21]

Som vi anfört i avsnitt 18.2.1 bedömer vi att våra direktiv som utgångspunkt inte innefattar ett uppdrag att lämna förslag som syftar till att stärka den brottsbekämpande verksamheten hos berörda myndigheter, även om utökade möjligheter till identifiering och verifiering av identiteten indirekt skulle kunna bidra till att motverka brottslighet som möjliggörs genom identitetsmissbruk, och främja att rätt personer lagförs. Möjligheten att identifiera en person – det vill säga att genom en en-till-många-jämförelse mot ett register få svar på frågan *Vem är du?* – kan vara av stor betydelse i den brottsbekämpande verksamhet som bedrivs av olika myndigheter (se avsnitt 18.2.1). Under vårt arbete har Polismyndigheten också anfört att man efterfrågar en möjlighet att kunna använda en-till-många-jämförelser i ett register som innehåller uppgifter om personer med samordningsnummer och om andra utlänningar, för att kunna identifiera personer som i olika sammanhang inte visar upp en giltig identitetshandling. Ett sådant behov är emellertid inte möjligt att tillgodose eller främja genom en möjlighet att biometriskt verifiera identiteten mot ett identitetsindex eller en identitetshandling, eftersom en sådan kontroll alltid innebär en en-till-en-jämförelse (se även avsnitt 7.2.1).

Det kan också noteras att Polismyndigheten har bedömts få möjlighet att använda biometriska uppgifter för jämförelser i register som förs av andra myndigheter – såsom Migrationsverkets register över fingeravtryck och fotografier[22] och uppgifter hos Skatteverket[23] – i mycket specifika situationer. I dessa fall krävs bland annat att en åklagare ska fatta beslut om sådan jämförelse, att jämförelse får ske endast under förundersökning beträffande vissa allvarliga brott samt att jämförelse får göras endast om det finns särskild anledning att anta att det är gärningsmannen som har avsatt fingeravtrycket eller förekommer på ansiktsbilden, och åtgärden är av synnerlig vikt för brottsutredningen. Även om verifiering av identitet inte kan anses lika integritetskänslig som ett sådant förfarande bör det, enligt vår mening, beaktas att Polismyndighetens möjligheter att göra biometriska jämförelser mot myndighetsregister som inte förs i brottsbe-

[21] *En modern och rättssäker förvaltning – ny förvaltningslag,* prop. 2016/17:180, s. 31.
[22] Prop. 2024/25:37, s. 130.
[23] *Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten*, prop. 2025/26:261, s. 85 f.

kämpande syfte är noga begränsade och förenade med särskilda, mycket specifika villkor.

Vi kan vidare konstatera att en uttrycklig rätt att kontrollera identiteten i brottsbekämpande verksamhet endast förekommer i relativt få fall. Polismyndigheten saknar en allmän rätt att kontrollera personers identitet. Utan att det framgår av lag får en polisman emellertid, om det är nödvändigt för att en tjänsteuppgift ska kunna fullgöras, fråga en person om hans eller hennes namn och hemvist. I de fall personen inte svarar eller lämnar vad som kan antas vara oriktiga uppgifter krävs lagstöd för att kontrollera uppgifterna vidare. En rätt till sådan kontroll finns i vissa fall enligt polislagen (1984:387). Av 14 § polislagen följer att om en okänd person anträffas av en polisman och det finns särskild anledning att anta att han eller hon är efterspanad eller efterlyst och med stöd av lag ska berövas friheten, får personen omhändertas för identifiering. Identitetskontroll kan också förekomma vid fordonsstopp enligt bestämmelsen i 22 § 4 polislagen. Vidare har polisen en möjlighet enligt 24 kap. 2 § rättegångsbalken att begära identitetsuppgifter från en enskild i de fall denne är misstänkt för brott. Som vi redogjort för i kapitel 7 har Polismyndigheten också en rätt att genomföra identitetskontroller i samband med gränskontroller och inre utlänningskontroller, bland annat i gränsnära områden; dessa utförs dock normalt inte inom ramen för den brottsbekämpande verksamheten utan som ett led i att upprätthålla en reglerad invandring. Även andra myndigheter med brottsbekämpande uppgifter har i vissa särskilt angivna fall en möjlighet att kontrollera identitet; enligt 5 kap. 8 § tullbefogenhetslagen (2024:710) är förare av transportmedel skyldiga att på begäran av en tulltjänsteman legitimera sig eller på annat godtagbart sätt styrka sin identitet.

I betänkandet *Åtgärder i gränsnära områden* anfördes att det finns ett behov av utökade möjligheter att kunna utföra identitetskontroller utan konkret misstanke om brott eller brottslighet, och Polismyndigheten framhöll då att en identitetskontroll är en väsentligt mindre ingripande åtgärd än exempelvis kroppsvisitation, vilket skulle kunna vara en alternativ åtgärd för att uppnå samma syfte. Vidare anfördes att identitetskontroller – till exempel kontroller av förare av fordon – kan ha ett stort värde för underrättelseverksamheten, men att det saknas en möjlighet att kontrollera passagerare i fordon och fotgängare. Slumpmässiga stickprovskontroller bedömdes kunna ha stor betydelse också för underrättelseverksamheten, genom att information

som kommer fram vid kontrollerna antas kunna bidra till att exempelvis mer träffsäkra profiler kan tas fram och ännu okänd gränsöverskridande brottslighet kan upptäckas och förhindras.[24]

Det är alltså tydligt reglerat i vilka särskilda situationer som identitetskontroller alls får genomföras i brottsbekämpande verksamhet. Vidare är det verksamhet som till sin natur har betydande inslag av myndighetsutövning och som kan omfatta rätt att använda tvångsåtgärder. Vi anser därför att det inom ramen för vårt uppdrag inte bör övervägas att utöka möjligheterna för myndigheter att inom ramen för brottsbekämpande verksamhet genomföra identitetskontroller, jämfört med de som finns i dag, exempelvis till att avse sådana situationer som lyftes fram i ovan nämnda betänkande. Att möjliggöra utökade kontroller av identiteten på fotgängare på det sätt som lyftes fram i ovan nämnda betänkande, eller av personer i allmänhet som en polisman kan påträffa, kräver noggranna överväganden ur rättssäkerhetssynpunkt, vilket talar starkt mot att detta bör göras inom ramen för vårt sakligt och tidsmässigt begränsade uppdrag.

Under vårt arbete har det även lyfts fram att det, för Polismyndighetens del, i första hand finns behov av att kunna identifiera och verifiera identiteten för tredjelandsmedborgare. Denna kategori av personer är i sig en förhållandevis begränsad grupp. Vi kan även konstatera att Polismyndigheten, genom flertalet lagstiftningsåtgärder under senare år, har fått och föreslås få utökade möjligheter att med hjälp av biometriska uppgifter kontrollera tredjelandsmedborgares identitet i samband med inresa till landet och under vistelsen i Sverige, bland annat genom kontroller enligt lagen (2023:474) om polisiära befogenheter i gränsnära områden och enligt 9 kap. utlänningslagen. Även om åtgärderna inte har ett direkt brottsbekämpande syfte anser vi att dessa möjligheter att kontrollera identiteten för tredjelandsmedborgare talar mot ett behov av motsvarande möjligheter i den brottsbekämpande verksamheten.

Att biometriskt kunna verifiera identitet mot ett identitetsindex eller en handling, i de fall då en identitetskontroll *får* genomföras enligt gällande regelverk, skulle enligt vår bedömning kunna öka tillförlitligheten av kontrollen och främja att användning av så kallade look-a-like-handlingar upptäcks. Den brottsbekämpande verksamheten är emellertid av särskilt ingripande karaktär och förändringar av den kräver särskilda överväganden. För att biometriska uppgifter

[24] SOU 2021:92, s. 218 f.

ska få behandlas – vid biometrisk verifiering av identitet mot ett identitetsindex eller en handling – i brottsbekämpande verksamhet krävs att det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen (se 2 kap. 12 § brottsdatalagen samt artikel 10 i dataskyddsdirektivet[25]). De situationer då biometrisk verifiering skulle kunna användas begränsas därför ytterligare. Införandet av en generell – och i förhållande till befintliga regelverk utökad – möjlighet för behöriga myndigheter att biometriskt verifiera identitet i brottsbekämpande verksamhet förutsätter enligt vår mening ingående överväganden avseende de brottsbekämpande myndigheternas olika verksamheter och behov.

Vad gäller biometrisk verifiering mot handlingar kan det vidare ifrågasättas om en eventuell möjlighet för brottsbekämpande myndigheter att kräva att den enskilde, på begäran, överlämnar en handling skulle få någon reell verkan i praktiken; till skillnad från ett ansökningsärende, där bristande medverkan eventuellt kan medföra att ansökan avvisas eller avslås med hänvisning till att det inte går att säkerställa att den avser rätt person, finns det som vi ser det inte motsvarande incitament för den enskilde att medverka i dessa avseenden i en situation av brottsbekämpande karaktär.

En rätt att vidta tvångsåtgärder för att möjliggöra biometrisk verifiering av identitet bör, enligt vår mening, inte övervägas (se avsnitt 21.5.3). För det fall myndigheter får en rätt att i brottsbekämpande verksamhet biometrisk verifiera identitet – mot antingen ett identitetsindex eller mot handlingar – finns det, som vi ser det, en risk för sammanblandning mellan myndighetens befogenheter att vidta olika åtgärder i olika situationer. Det kan vidare framstå som oklart för den enskilde, som kanske är misstänkt för ett brott, vilka åtgärder han eller hon är skyldig att medverka till och när det finns en rättslig möjlighet att vägra att medverka till ett genomförande av åtgärden.

Sett i ljuset av vårt övergripande uppdrag och den tidsram vi har till vårt förfogande anser vid därför sammantaget att eventuella utökade möjligheter för myndigheter att i brottsbekämpande verksamhet verifiera identitet med hjälp av biometriska uppgifter mot ett identitetsindex eller en handling bör utredas i annan ordning.

[25] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016.

21.5 Verifiering med hjälp av biometriska uppgifter

Vår redogörelse för identitetsmissbruk och dess konsekvenser i kapitel 9 samt vår utvärdering av tänkbara åtgärder för säkrare verifiering av identitet i kapitel 10 visar, enligt vår mening, att myndigheters behov av att kunna verifiera identitet på ett annat sätt än i dag är mycket stort. Frågan är i vilken utsträckning myndigheters verifiering av identitet bör kunna göras med hjälp av biometriska uppgifter genom en jämförelse mot uppgifter i ett centralt register, såsom ett identitetsindex, alternativt mot handlingar, inom ramen för en sådan mer generell möjlighet som vi överväger.

Myndigheter bör som utgångspunkt ha möjlighet att verifiera identitet genom kontroll mot biometriska uppgifter när det finns ett sådant behov i myndighetens verksamhet. Det är enligt vår bedömning emellertid inte lämpligt att låta myndigheter helt fritt avgöra när en persons identitet ska verifieras genom kontroll med hjälp av biometriska uppgifter och det bör inte finnas en generell möjlighet för myndigheter att verifiera identitet i samtliga situationer där myndigheten anser att det finns ett behov. Behovet måste, som vi ser det, vara av en viss styrka för att åtgärden att verifiera identiteten biometriskt ska anses vara proportionerlig. Det är visserligen rimligt att anta att en myndighet inte skulle verifiera identitet biometriskt genom kontroll mot ett index eller en handling i onödan. Vi anser dock att såväl myndigheternas användning av ett index som av en handling för biometrisk verifiering behöver begränsas till vissa situationer, för att skapa förutsebarhet och tydlighet – för såväl myndigheter som enskilda – om under vilka förutsättningar en sådan verifiering ska vara tillåten.

Det är inte möjligt att inom ramen för vårt uppdrag utreda vitt skilda myndigheters olika behov av att kunna verifiera identitet i olika situationer. Ett regelverk för sådana kontroller behöver därför innehålla tillräckligt generellt utformade bestämmelser, men som på lämpligt sätt begränsar och specificerar under vilka förutsättningar det bör vara möjligt för myndigheter att biometriskt verifiera identitet mot ett identitetsindex eller mot en handling. Sådana bestämmelser behöver utformas på ett sätt som möjliggör verifiering i situationer då det som utgångspunkt kan anses vara proportionerligt att en biometrisk verifiering görs, och som i möjligaste mån förhindrar verifiering i situationer då det framstår som för ingripande i förhållande

till myndighetens behov av att kontrollera identitet. Att hitta rätt balans i detta avseende medför vissa utmaningar.

Utgångspunkten bör enligt vår bedömning vara att myndigheternas behov av att säkert kunna verifiera identitet tillgodoses i så stor utsträckning som möjligt, och det är av naturliga skäl myndigheten själv som bäst kan avgöra när det finns ett behov av säker verifiering i form av biometrisk sådan i dess verksamhet. Biometrisk verifiering av identitet bör dock inte användas slentrianmässigt, till exempel när personen är känd av myndigheten eller när en persons identitet inte är relevant för att myndigheten ska kunna agera korrekt i den aktuella situationen. Det kan i sistnämnda fall exempelvis vara fråga om åtgärder som en myndighet vidtar inom ramen för sin serviceskyldighet och som inte innefattar någon form av myndighetsutövning.

21.5.1 Handläggning av ett ärende enligt förvaltningslagen

Vår bedömning

En myndighet bör få använda biometriska uppgifter för att verifiera identitet om det är nödvändigt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde.

Många myndigheters verksamhet består i mycket stor utsträckning av ärendehandläggning. Var gränsen går mellan ärendehandläggning och annan förvaltningsverksamhet, så kallat faktiskt handlade, får avgöras från myndighet till myndighet. I den del av en myndighets verksamhet som består av handläggning av ärenden får det, enligt vår bedömning, generellt sett anses finnas ett stort behov för myndigheten att säkert kunna verifiera en persons identitet. Utan vetskap om vem en person är kan myndigheten som utgångspunkt inte ta ställning till exempelvis om personen har rätt att få en socialförsäkringsförmån eller bör beviljas serveringstillstånd enligt alkohollagen. Det bör därmed utvärderas under vilka omständigheter en myndighet bör få verifiera identitet biometriskt vid handläggningen av ett ärende. En sådan utvärdering omfattar dels vilka typer av ärenden som bör aktualiseras, dels under vilka förutsättningar en biometrisk verifiering ska få göras i sådana ärenden.

Ärenden enligt förvaltningslagen

Enligt 1 § förvaltningslagen gäller lagen för handläggning av ärenden hos förvaltningsmyndigheterna och handläggning av förvaltningsärenden hos domstolarna. Regleringen innebär därmed att en mycket stor del av den offentliga förvaltningen berörs av förvaltningslagen. Bestämmelserna i 5–8 §§ om grunderna för god förvaltning gäller även i annan förvaltningsverksamhet hos förvaltningsmyndigheter och domstolar. Med uttrycket förvaltningsmyndighet avses samma typ av organ som i regeringsformen, det vill säga de organ som ingår i den offentligrättsliga statliga och kommunala organisationen. En gränsdragning mellan domstolar och förvaltningsmyndigheter kan göras på i huvudsak organisatoriska och funktionella grunder. Medan förvaltningsmyndigheter är organ vars huvudsakliga uppgift är att sköta den offentliga förvaltningen är domstolarna organ som har till huvudsaklig uppgift att ägna sig åt rättskipande verksamhet (avgöra rättstvister, tillämpa strafflag och pröva rättsfrågor).[26]

Vissa undantag från tillämpningsområdet gäller för kommunala ärenden där besluten laglighetsprövas (2 §) och i brottsbekämpande verksamhet hos Kustbevakningen, Polismyndigheten, Skatteverket, Säkerhetspolisen, Tullverket eller en åklagarmyndighet (3 §). I dessa fall ska merparten av bestämmelserna i förvaltningslagen inte tillämpas. Förvaltningslagen är vidare subsidiär (4 §), det vill säga en föreskrift som har tagits in i en annan lag eller i en förordning ska tillämpas i stället för förvaltningslagen om den särskilda föreskriften avviker från förvaltningslagen i något hänseende som regleras i lagen.

Vi bedömer att en myndighet, som utgångspunkt, bör ha möjlighet att verifiera identitet biometriskt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Det får vid handläggningen av denna typ av ärenden generellt sett anses finnas ett stort behov för myndigheten att kunna kontrollera att en person är den han eller hon utger sig för att vara. Att tillåta biometrisk verifiering av identitet vid handläggningen av ett ärende som omfattas av tillämpningsområdet för förvaltningslagen medför vidare att sådan verifiering blir möjlig i ett stort antal olika ärenden, hos ett mycket stort antal myndigheter, vilket främjar möjligheterna för det allmänna att motverka identitetsmissbruk. Med hänsyn till de ytterligare villkor som enligt vår bedömning bör vara uppfyllda för att en biomet-

[26] Prop. 2016/17:180, s. 25 f.

risk verifiering ska vara tillåten (se nedan i detta avsnitt) anser vi att en så omfattande möjlighet till sådan verifiering är motiverad och proportionerlig (se avsnitt 21.7.3).

Med hänsyn till att förvaltningslagen är subsidiär kan det finnas avvikande bestämmelser i annan lag som ska tillämpas i stället. Även i de fall det finns verksamhetsspecifika bestämmelser i annat regelverk som reglerar handläggningen av det aktuella ärendet – till exempel skatteförfarandelagen (2011:1244), socialtjänstlagen (2025:400) och socialförsäkringsbalken – är det dock fråga om ett ärende som omfattas av tillämpningsområdet för förvaltningslagen.

Vad som kännetecknar ett ärende framgår inte av någon särskild bestämmelse i förvaltningslagen. Kännetecknande är emellertid att ett ärende regelmässigt avslutas genom ett uttalande från myndighetens sida som är avsett att få faktiska verkningar för en mottagare i det enskilda fallet. Ett ärende avslutas genom ett beslut av något slag. Vid bedömning av frågan om en myndighets ställningstagande är att anse som ett beslut i denna mening är det uttalandets syfte och innehåll som avgör dess karaktär, inte dess yttre form. Uttrycket handläggning innefattar alla åtgärder som en myndighet vidtar från det att ett ärende inleds till dess att det avslutas.[27]

Ett ärende hos en myndighet inleds oftast av den enskilde genom en ansökan, anmälan eller annan framställning, på det sätt som avses i 19 § förvaltningslagen. I en sådan situation handlar det vanligen om att den enskilde vill att myndigheten ska vidta någon form av åtgärd rörande honom eller henne, till exempel bevilja en förmån eller ett tillstånd. Det framstår som rimligt att myndigheten i dessa fall bör ha möjlighet att – på ett säkert sätt – bekräfta att den enskilde är den han eller hon påstår sig vara, för att kunna fatta ett korrekt beslut i ärendet. En myndighet skulle emellertid även kunna ha behov av att verifiera identitet biometriskt vid handläggningen av ett ärende som inleds av myndigheten själv, av en annan myndighet eller av en annan enskild än den som ärendet primärt berör. En enskild kan till exempel göra en anmälan till Försäkringskassan om misstänkt fusk. Om Försäkringskassan i en sådan situation inleder ett ärende kan det antas vara framför allt identitet hos den som anmälan avser som behöver kontrolleras, inte anmälarens identitet. Integritetsintrånget för den enskilde får anses vara större i en situation där denne inte initierat kontakten med myndigheten och kanske inte heller är intresserad

[27] Prop. 2016/17:180, s. 286.

av att ha kontakt med myndigheten. Myndighetens behov av säker verifiering av identitet kan dock vara lika stort vid handläggningen av ett sådant ärende, och säker verifiering kan vara en förutsättning för att myndigheten ska kunna fatta ett korrekt beslut i ärendet.

Biometrisk verifiering av identitet mot ett identitetsindex eller mot en handling bör enligt vår mening alltså vara möjlig för en myndighet vid handläggning av ett ärende som omfattas av tillämpningsområdet för förvaltningslagen oavsett anledningen till att ärendet inletts. Detta eftersom en myndighet som utgångspunkt kan antas ha ett befogat intresse av att verifiera identitet biometriskt vid handläggningen av ett sådant ärende.

Andra ärenden bör inte omfattas

Att förvaltningslagen enligt 1 § gäller i förvaltningsverksamhet innebär att tillämpningsområdet är mycket omfattande. Fråga är om det bör vara möjligt för en myndighet att biometriskt verifiera identitet – mot ett identitetsindex eller mot en handling – vid handläggningen av andra ärenden än sådana som omfattas av förvaltningslagens tillämpningsområde.

Vi har i avsnitt 21.4 bedömt att en möjlighet för myndigheter att i brottsbekämpande verksamhet biometriskt verifiera identitet bör utredas i annan ordning. Det innebär att utredningen inte bör lämna förslag som medför att biometrisk verifiering av identitet är tillåten till exempel inom ramen för en förundersökning eller vid handläggningen av ett brottmål i allmän domstol. Såväl de allmänna domstolarna som förvaltningsdomstolarna handlägger emellertid ärenden och mål som varken omfattas av förvaltningslagens tillämpningsområde eller anses vara en del av den brottsbekämpande verksamheten.

För de allmänna domstolarnas del kan det bland annat bli aktuellt att tillämpa lagen (1996:242) om domstolsärenden (ärendelagen), som gäller handläggningen i tingsrätt, hovrätt och Högsta domstolen av sådana rättsvårdsärenden som ska tas upp av en tingsrätt och som inte ska handläggas enligt rättegångsbalken. Vid handläggningen av tvistemål tillämpar de allmänna domstolarna främst det regelverk i rättegångsbalken som tar sikte på just tvistemål. För förvaltningsdomstolarna gäller förvaltningsprocesslagen (1971:291) vid rättsskipning i Högsta förvaltningsdomstolen, kammarrätt och förvaltningsrätt.

Domstolarnas verksamhet och handläggningen av mål och ärenden i dessa avseenden har en annan karaktär än förvaltningsmyndigheternas handläggning av ärenden. Vad gäller mål och ärenden som handläggs enligt ärendelagen och förvaltningsprocesslagen är det fråga om överklagande av en förvaltningsmyndighets beslut. För det fall det finns oklarheter avseende en persons identitet vid handläggningen av ärendet hos förvaltningsmyndigheten kommer den myndigheten, enligt våra överväganden, att ha möjlighet att biometriskt verifiera identiteten. Det bör, enligt vår bedömning, endast i undantagsfall finnas behov av att i domstol kunna verifiera en persons identitet vid handläggningen av ett ärende enligt ärendelagen eller ett mål enligt förvaltningsprocesslagen. Något direkt behov av att kunna verifiera en persons identitet biometriskt vid handläggning av ett tvistemål kan vi inte heller se, även om tingsrätten normalt är första instans i dessa fall. Parterna i denna typ av mål är ofta kända för varandra och det kan antas sällan finnas incitament att försöka vilseleda andra om identiteten i dessa sammanhang. Vi kan vidare konstatera att sådana eventuella behov i viss mån skulle kunna tillgodoses genom den möjlighet att biometriskt verifiera identitet som vi redogör för i avsnitt 21.5.2.

Till de allmänna domstolarna räknas tingsrätter, hovrätter och Högsta domstolen. Vissa domstolar utgör en del av en tingsrätt eller hovrätt; här kan nämnas patent- och marknadsdomstolarna, som tillämpar lagen (2016:188) om patent- och marknadsdomstolar avseende handläggningen av mål och ärenden, samt mark- och miljödomstolarna, som tillämpar lagen (2010:921) om mark- och miljödomstolarna avseende handläggningen av mål och ärenden. Det finns också specialdomstolar, där Arbetsdomstolen kan nämnas; lagen (1974:371) om rättegången i arbetstvister tillämpas på rättegången i tvister mellan arbetsgivare och arbetstagare. Inte heller vad gäller dessa – eller andra – ärenden och mål i domstolarna ser vi något direkt behov av att kunna verifiera en persons identitet biometriskt. Precis som vad gäller i tvistemål är parterna ofta kända för varandra i dessa typer av mål och ärenden och det kan antas sällan finnas incitament att försöka vilseleda en domstol om identiteten.

Mot den här bakgrunden bedömer vi att behovet av att kunna verifiera identitet biometriskt i mål och ärenden hos domstolarna får anses begränsat. Det har enligt vår mening inte heller kommit fram några andra ärendeslag än sådana som omfattas av förvaltningslagens tillämp-

ningsområde som det generellt sett kan anses finnas ett behov av att kunna verifiera identitet biometriskt i. Vi anser därmed att en möjlighet att verifiera en persons identitet biometriskt vid handläggningen av ett ärende bör kopplas endast till ärenden som omfattas av förvaltningslagens tillämpningsområde.

Biometrisk verifiering ska vara nödvändig

För att förhindra biometrisk verifiering när det inte behövs för handläggningen av ett ärende bör det krävas att ytterligare rekvisit är uppfyllda för att sådan verifiering ska vara tillåten. Med tanke på det stora antalet myndigheter som kan komma att få möjlighet att verifiera identitet biometriskt, och det ännu större antalet ärendeslag som skulle kunna föranleda sådan verifiering, är det inte möjligt att – inom ramen för vårt uppdrag – ta ställning till under vilka närmare förutsättningar en biometrisk verifiering bör göras i olika ärendeslag, till exempel ett socialförsäkringsärende hos Försäkringskassan, ett ärende om godkännande för F-skatt hos Skatteverket eller ett ärende om körkort hos Transportstyrelsen. Det bör, enligt vår mening, emellertid på ett generellt sätt regleras vad som ska krävas för biometrisk verifiering. Detta för att förhindra att sådan verifiering görs mer eller mindre slentrianmässigt vid handläggning av ärenden, utan att det finns ett faktiskt behov.

Ett tänkbart rekvisit för biometrisk verifiering är att *identiteten är av betydelse för handläggningen av ärendet*. Vi bedömer att så kan anses vara fallet i den stora majoriteten ärenden som handläggs av olika myndigheter; utan vetskap om vem som till exempel ansökt om en förmån eller gjort en anmälan om bosättning hos Försäkringskassan kan det vara svårt för myndigheten att handlägga ärendet korrekt. Det framgår även av 19 § förvaltningslagen att en framställan från den enskilde ska innehålla uppgifter om den enskildes identitet, vilket tydliggör detta. Det förekommer emellertid även att myndigheter handlägger ärenden av sådan karaktär att enskildas identitet inte är av direkt betydelse. Som ett exempel kan nämnas en sådan miljöbedömning som ska göras enligt 6 kap. miljöbalken. Ett villkor om att identiteten ska vara av betydelse för handläggningen av ärendet skulle utesluta att en biometrisk kontroll av identiteten kan göras vid handläggningen av sådana ärenden. Det skulle enligt vår mening

inte heller vara lämpligt att i lag förtydliga under vilka förutsättningar identiteten ska anses vara av betydelse för handläggningen av ett ärende. Med ett sådant villkor skulle det i stället ankomma på myndigheten att utifrån dess verksamhet utvärdera under vilka förutsättningar identiteten ska anses vara av betydelse och eventuellt ta fram riktlinjer eller liknande för användning av en möjlighet att verifiera identitet biometriskt.

I ärenden som innefattar ett uttryckligt krav på att identiteten ska styrkas, som innebär att den enskilde ska styrka en viss behörighet, eller som avser beviljande av en förmån av något slag för en person bör det visserligen som utgångspunkt kunna antas att identiteten är av central betydelse. Ett villkor om att identiteten ska vara av betydelse för handläggningen av ett ärende skulle emellertid ge myndigheterna ett mycket stort skönsmässigt utrymme att bedöma när så ska anses vara fallet i dess verksamhet. Vidare möjliggör ett sådant villkor – enligt ordalydelsen – biometrisk verifiering av identitet även i de fall då det inte finns något egentligt behov av en biometrisk verifiering, till exempel när personen är känd av myndigheten sedan tidigare. Även om det är rimligt att anta att myndigheter inte kommer att verifiera en persons identitet biometriskt när det inte behövs anser vi att rekvisitet att identiteten ska vara av betydelse inte är lämpligt.

Det skulle i stället kunna övervägas att biometrisk verifiering förutsätter att det inte *med tillräcklig säkerhet* går att verifiera identiteten på något annat sätt än genom en biometrisk kontroll. Ett sådant villkor skulle signalera att andra åtgärder för att verifiera identiteten ska vidtas i stället, om sådana åtgärder bedöms tillräckliga i det enskilda fallet. Ordalydelsen i ett sådant villkor kräver emellertid inte att andra åtgärder också faktiskt har vidtagits först. Oaktat detta bedömer vi att ett villkor som föreskriver att biometrisk verifiering är tillåten endast när andra verifieringsåtgärder är otillräckliga riskerar att i för stor utsträckning begränsa möjligheterna att använda biometrisk verifiering, och ger intrycket av att det i det enskilda fallet måste motiveras varför en annan typ av kontroll inte är tillräcklig. Behovet av verifiering skulle därmed också kunna ifrågasättas. Rekvisitet med tillräcklig säkerhet kan antas skapa tillämpningsproblem och osäkerhet kring när en biometrisk verifiering är tillåten. Vidare är det i många situationer inte möjligt för en myndighet att upptäcka identitetsmissbruk utan biometrisk verifiering och därmed är det svårt att i förväg veta när verifiering på annat sätt är tillräcklig. Även i ett ärende där

den enskilde till exempel åberopar en giltig identitetshandling – och en okulär jämförelse av personen och ansiktsbilden på handlingen inte ger anledning att misstänka några oegentligheter – kan det vara fråga om identitetsmissbruk som endast kan upptäckas genom en biometrisk verifiering.

För att ett system med biometrisk verifiering av identitet ska fylla en funktion i att motverka identitetsmissbruk och faktiskt komma till användning i mer än ett relativt begränsat antal situationer anser vi att myndigheter, vid handläggningen av ett ärende, bör kunna verifiera identitet biometriskt även om det inte kommit fram någon särskild omständighet i det enskilda ärendet som ger anledning att anta att den enskilde försöker vilseleda myndigheten om sin identitet. Det bör, enligt vår mening, till exempel vara möjligt för en myndighet att göra slumpmässiga biometriska kontroller av identitet i ärendeslag där myndigheten generellt sett har bedömt att det finns en risk för identitetsmissbruk. Även om identitetsmissbruk kan komma att uppmärksammas endast i en liten andel av sådana slumpmässiga kontroller kan de ha en avskräckande effekt och på så sätt motverka identitetsmissbruk.

Vi bedömer att möjligheten att verifiera identitet biometriskt vid handläggningen av ett ärende bör vara beroende av att detta är *nödvändig* vid handläggningen. Det bör, enligt vår mening, ankomma på den myndighet som handlägger ärenden av ett visst slag att avgöra om det är nödvändigt med en biometrisk verifiering av en persons identitet. För det fall en myndighet bedömer att det finns ett sådant behov får det, som utgångspunkt, anses vara nödvändigt med en sådan verifiering. Myndigheten behöver dock kunna peka på någon konkret omständighet som innebär att användning av biometriska uppgifter är nödvändig – exempelvis att en okulär kontroll av en identitetshandling av något slag inte är tillräcklig eller möjlig att genomföra – för att uppnå ändamålet med kontrollen. Sådana omständigheter kan som vi ser det både finnas på en mer övergripande nivå och hänföra sig till omständigheter i det enskilda fallet. Med detta menar vi att det ska vara nödvändigt att verifiera personens identitet biometriskt till exempel för att myndigheten bedömer att ärendet är av sådan karaktär att en säker verifiering behövs för att säkerställa en korrekt hantering. Biometrisk verifiering skulle även kunna anses vara nödvändig när ett ärende har inletts på distans genom att den enskilde använt en e-legitimation – till exempel BankID –

för att skriva under en ansökan; i sådana situationer görs normalt inga identitetskontroller, och en okulär kontroll av en identitetshandling kan av naturliga skäl inte genomföras, om inte den enskilde vid ett senare tillfälle besöker myndigheten på plats. I ärenden som inleds på distans utgör biometrisk verifiering – i form av en sådan verifieringsprocess som vi beskriver i avsnitt 27.4 – därför normalt den enda rimliga metoden att uppnå ändamålet att verifiera identiteten på ett säkert sätt. Sådan verifiering skulle därför, som vi ser det, normalt kunna anses nödvändig vid handläggningen av ärenden som inletts på distans, om säker verifiering av identitet är av betydelse vid handläggningen av det aktuella ärendet. Det bör, som vi ser det, även kunna anses vara nödvändigt med stickprovskontroller, under förutsättning att ärendeslaget i sig är sådant att säker verifiering av identitet kan anses vara av betydelse vid handläggningen av det aktuella ärendeslaget.

Det bör alltså inte krävas att det i det enskilda ärendet finns anledning att misstänka att den enskilde försöker vilseleda myndigheten om sin identitet. Myndigheten måste däremot, som vi nämnt ovan, kunna visa att en biometrisk verifiering är nödvändig, exempelvis på grund av att myndigheten har fått indikationer på att det förekommer identitetsmissbruk i ett visst ärendeslag. Vid en kontroll av identitet på plats kan det även vara fråga om att den tjänsteman som möter personen har anledning att misstänka att handlingen är felaktig eller att någon annans identitetshandling används. I de fall en myndighet har personlig kännedom om personen i fråga kan det, enligt vår mening, dock inte anses vara nödvändigt att biometriskt verifiera personens identitet. Som exempel kan nämnas en person som regelbundet får ekonomiskt bistånd från socialtjänsten och som träffat handläggaren av ärendet vid upprepade tillfällen.

Rekvisitet nödvändig är avsett att ha samma betydelse som det dataskyddsrättsliga begreppet nödvändig. Enligt skäl 39 till dataskyddsförordningen bör personuppgifter bara behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.[28] EU-domstolen har uttryckt det så att kravet på nödvändighet inte är uppfyllt när det eftersträvade målet rimligen kan uppnås på ett lika effektivt sätt genom andra medel som i mindre utsträckning inskränker de registrerades grundläggande rättigheter. Begreppet nödvändig inne-

[28] Se avgörandena i mål C-439/19, *Latvijas Repbublikas Saeima*, punkt 110, mål C-252/21, *Meta Platforms m.fl.*, punkt 108 och mål C-26/22 och C-64/22, *SCHUFA Holding*, punkt 77.

bär däremot inte ett krav på att behandlingen av personuppgifter ska vara oundgänglig, utan att bara sådana uppgifter som behövs får behandlas.[29]

I nationella bestämmelser om personuppgiftsbehandling anges ibland att behandlingen ska *behövas* till exempel för ett visst ändamål och ibland att den ska vara *nödvändig*. I detta sammanhang anses de båda uttryckssätten vara synonyma.[30] I propositionen *Framtidens dataskydd vid Skatteverket, Tullverket och Kronofogdemyndigheten* uttalade regeringen att det är lämpligt att använda begreppet *nödvändig* i den nationella lagstiftningen, även om någon ändring i sak i förhållande till begreppet *behövs* i nuvarande ändamålsbestämmelser inte är avsedd. Vidare uttalades att kravet på nödvändighet inte innebär ett krav på att behandlingsåtgärden ska vara oundgänglig. En bestämmelse som anger att behandlingen ska vara nödvändig för att utföra verksamhet inom de föreslagna dataskyddslagarnas respektive materiella tillämpningsområde hindrar, enligt regeringen, dock myndigheterna från att behandla personuppgifter som inte kan hänföras till deras författningsreglerade uppgifter. [31]

Det blir i det här avseendet fråga om en form av kombinationsreglering som inte bara avser förutsättningarna för myndigheter att använda biometrisk verifiering, utan även begränsar myndigheters möjlighet att behandla personuppgifter; det senare för att skapa förenlighet med artikel 6 och 9 i dataskyddsförordningen. Biometrisk verifiering av identitet mot ett identitetsindex eller mot en handling är, enligt vår mening, att betrakta som en specifik utredningsåtgärd som får användas av en myndighet under vissa förutsättningar. Vid en biometrisk verifiering aktualiseras endast behandling av ett fåtal personuppgifter och uppgifterna behandlas endast i den situationen; verifieringen föranleder ingen ytterligare behandling av uppgifterna i myndighetens verksamhet i övrigt. Genom att knyta den materiella bestämmelsen om verifiering av identitet till det dataskyddsrättsliga rekvisitet nödvändig säkerställs att biometrisk verifiering av identitet får användas endast när det behövs för att uppnå ändamålet med den, det vill säga – i den situation vi nu utvärderar – när det behövs för att säkert verifiera personens identitet vid handläggningen av ett ärende enligt förvaltningslagen. Vid reglering av mer omfattande verksamhet

[29] *Ny dataskyddslag,* prop. 2017/18:105, s. 189 och 194.
[30] *Behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering,* prop. 2011/12:176, s. 30.
[31] Prop. 2025/26:88, s. 132.

är det emellertid vanligt att det regelverk som specificerar myndighetens uppgifter och förutsättningarna för denna är separerat från regelverket med bestämmelser om personuppgiftsbehandling. Som exempel kan nämnas utlänningslagen och utlänningsdatalagen (2016:27) samt socialtjänstlagen och lagen (2001:454) om behandling av personuppgifter inom socialtjänsten.

21.5.2 Identitetskontroller i annat fall

Vår bedömning

En myndighet bör få använda biometriska uppgifter för att verifiera identitet – i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde – om det är nödvändigt när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller.

Inte all verksamhet som bedrivs av en myndighet avser ärendehandläggning. Många myndigheter har så kallad faktiskt verksamhet, till exempel rådgivning och annan service, uppföljning eller olika former av samverkan utan ärendeanknytning. En principiell skillnad mellan ärendehandläggning och faktiskt handlande är att handläggningen av ett ärende avslutas med ett beslut av något slag, medan ett faktiskt handlande karaktäriseras av att myndigheten i praktiken vidtar en viss faktisk åtgärd.[32] En möjlighet för myndigheter att verifiera identitet biometriskt i den faktiska verksamheten bör som vi ser det utvärderas. För att en sådan möjlighet ska vara motiverad från integritetssynpunkt krävs det, enligt vår mening, att det finns ett visst mått av förutsebarhet och tydlighet vad gäller när en myndighet har rätt att genomföra en biometrisk verifiering av identitet. Myndigheters användning av biometrisk verifiering får inte framstå som godtycklig och regelverket bör ge enskilda möjlighet att få en uppfattning om när en myndighet i så fall får begära sådan verifiering.

[32] Prop. 2016/17:180, s. 24.

Identitetskontroller i annat fall än vid handläggningen av ett ärende enligt förvaltningslagen

Det förekommer att myndigheter kontrollerar en persons identitet, till exempel genom en okulär kontroll av en identitetshandling, i olika sammanhang utan att den föranleds av handläggningen av ett specifikt ärende som omfattas av tillämpningsområdet för förvaltningslagen. Som exempel kan nämnas den identitetskontroll som genomförs med stöd av 8 kap. 6 § vallagen (2005:837) vid röstning i val. Ett annan exempel på identitetskontroller som inte är knutna till handläggningen av ett ärende är sådana kontroller som genomförs av personer som söker vård, för att kunna garantera trygghet och säkerhet i alla kontakter med vårdgivare.[33] Vidare har huvudmannen, enligt 6 a kap. 4 § skollagen (2010:800) en skyldighet att förhindra att obehöriga personer får tillträde till en förskola, skola eller ett fritidshem under tid när verksamheten pågår och kan behöva genomföra en identitetskontroll med anledning av det. Om personen visar sig vara behörig föranleder en sådan kontroll inga ytterligare åtgärder. Ett annat exempel som kan nämnas är identitetskontroller som genomförs i samband med det så kallade högskoleprovet.

Vi bedömer att myndigheter som redan i dag utför identitetskontroller inom ramen för sin verksamhet, och därmed har ett behov av att verifiera personers identitet, bör få möjlighet att under vissa förutsättningar göra det på ett säkrare sätt, det vill säga genom användning av biometriska uppgifter. Att det ska vara fråga om identitetskontroller inom ramen för myndighetens verksamhet innebär att genomförandet av identitetskontrollen ska föranledas av den verksamhet myndigheten bedriver. Det behöver inte finnas ett uttryckligt rättsligt stöd för myndigheten att genomföra identitetskontroller, men myndigheten får givetvis inte agera utanför sitt uppdrag. Det regelverk vi överväger ska, enligt vår mening, inte kunna åberopas som självständig rättslig grund för att genomföra en identitetskontroll på det sätt vi avser i sammanhanget. Om en myndighet bedömer att det finns rättsliga förutsättningar för att genomföra en identitetskontroll, inom ramen för dess verksamhet, ska kontrollen dock kunna kompletteras med en jämförelse av biometriska uppgifter, med stöd av det nya regelverket.

[33] https://www.vardhandboken.se/arbetssatt-och-ansvar/ansvar-och-regelverk/identifikation/oversikt/, hämtad 2026-03-16.

Det handlar alltså om situationer där myndigheten har ett behov av att verifiera en persons identitet, framför allt för att kunna bedriva sin faktiska verksamhet på ett korrekt och ändamålsenligt sätt, och där personen som utgångspunkt kan förvänta sig att myndigheten kommer att kontrollera hans eller hennes identitet, vanligen genom att begära att han eller hon visar upp en fysisk identitetshandling eller en annan handling som innehåller identitetsuppgifter. Att en myndighet i en sådan situation även har möjlighet att verifiera identiteten biometriskt framstår, enligt vår mening, som tillräckligt förutsebart för den enskilde.

Biometrisk verifiering ska vara nödvändig

Vad gäller biometrisk verifiering av identitet vid handläggningen av ett ärende som omfattas av tillämpningsområdet för förvaltningslagen har vi i avsnitt 21.5.1 bedömt att en sådan verifiering bör vara *nödvändig* vid handläggningen för att få genomföras och begreppet är avsett att ha samma betydelse som det dataskyddsrättsliga begreppet. Fråga är om det samma bör gälla som villkor för biometrisk verifiering när en myndighet, inom ramen för sin verksamhet, genomför identitetskontroller.

Vid handläggningen av ett ärende som omfattas av tillämpningsområdet för förvaltningslagen kommer det i många fall att vara fråga om en verifiering på distans; få ärenden hos förvaltningsmyndigheter inleds i dag på plats hos en myndighet. När personen i fråga till exempel loggat in på Mina sidor hos Försäkringskassan med en e-legitimation finns det i praktiken inget annat sätt för myndigheten att säkerställa att personen som använder e-legitimationen är den person som e-legitimationen utfärdats för än en biometrisk verifiering (se även avsnitt 19.3.6 avseende bärare av e-legitimationer). Det innebär, som vi ser det, att det ofta kommer att finnas stöd för en biometrisk verifiering i dessa fall.

Vid biometrisk verifiering när en myndighet i annat fall än vid än handläggningen av ett ärende enligt förvaltningslagen genomför en identitetskontroll kommer det i stället i princip uteslutande att vara fråga om en verifiering som genomförs när personen i fråga fysiskt möter en representant för myndigheten. I dessa fall finns det därför, som utgångspunkt, en möjlighet att göra en okulär kontroll av en

identitetshandling eller – i avsaknad av en sådan handling – till exempel ett uppehållstillståndskort. Det går också i vissa fall att konstatera att det är en person som myndigheten tidigare har mött och vars identitet man därför har god kännedom om. Vidare handlar det, som utgångspunkt, om att ta reda på om en person är den han eller hon utger sig för att vara, i myndighetens faktiska verksamhet. Det kan givetvis finnas anledning för en person att försöka vilseleda en myndighet om sin identitet även i en sådan situation, men vi bedömer att incitamentet vanligen är svagare än vid handläggningen av ett ärende, inte minst då risken för upptäckt kan antas vara större när en person möter en företrädare för myndigheten än när kontakten sker helt på distans.

En myndighet måste naturligtvis alltid agera inom ramen för sitt uppdrag och sin verksamhet. Det är emellertid inte alltid lika tydligt – särskilt för den enskilde – vilka åtgärder en myndighet får vidta inom ramen för den så kallade faktiska verksamheten som vilka utredningsåtgärder myndigheten får vidta vid handläggningen av ett ärende. Det finns som utgångspunkt inte heller någon omedelbar möjlighet att överklaga en myndighets agerande i den faktiska verksamheten, med hänsyn till att sådant agerande sällan utmynnar i ett förvaltningsbeslut, om inte den enskilde särskilt efterfrågar detta. Även med hänsyn till att det kan vara svårare att på ett tydligt sätt definiera myndigheters faktiska verksamhet, anser vi att en begränsning i form av att biometrisk verifiering endast bör få genomföras när det är nödvändigt är lämplig också när en identitetskontroll genomförs, på samma sätt som beskrivs i föregående avsnitt (21.5.1).

Även i den faktiska verksamheten kan frågan om när det är nödvändigt att använda biometrisk verifiering bero på såväl mer generella omständigheter som omständigheter i det enskilda fallet. Det ligger exempelvis – enligt vår mening – nära till hands att anse att biometrisk verifiering regelmässigt kan vara nödvändig vid identitetskontroller i verksamheter där identitetsmissbruk kan innebära direkta risker i verksamheten eller för andra, till exempel för att kunna garantera patientsäkerheten i vården. En viss myndighet kan också tillfälligt anse sig behöva genomföra förstärka identitetskontroller, till exempel på grund av en hotbild mot myndigheten, mot anställda eller mot enskilda som vistas i verksamheten. Omständigheter i det enskilda fallet skulle kunna vara att en okulär kontroll av en identitetshandling ger misstankar om att någons identitet utnyttjas. Myndigheten

måste alltså också i den faktiska verksamheten kunna peka på någon konkret omständighet som innebär att biometrisk verifiering är nödvändig; slentrianmässiga kontroller med hjälp av biometriska uppgifter, som utan någon direkt anledning i praktiken ersätter den typ av identitetskontroll som annars genomförs i verksamheteten, bör alltså inte kunna användas. Den möjlighet till biometrisk verifiering som vi anser bör tillåtas i den faktiska verksamheten ska ses som en kompletterande utredningsåtgärd, inte som en självständig metod för myndigheter att genomföra identitetskontroller.

Mot denna bakgrund anser vi därmed att även biometrisk verifiering av identitet när myndigheten genomför identitetskontroller – i annat fall än vid än handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde – bör få genomföras om det är *nödvändigt* att verifiera innehavarens identitet på detta sätt. Utifrån de olika förutsättningarna i myndigheters verksamhet med ärendehandläggning enligt förvaltningslagen respektive i deras faktiska verksamhet, kan bedömningen av vad som är nödvändigt i den aktuella situationen dock, som vi pekat på ovan, komma att skilja sig åt.

21.5.3 En rätt att vidta tvångsåtgärder bör inte övervägas

Vår bedömning

En rätt att vidta tvångsåtgärder för att möjliggöra biometrisk verifiering av identitet bör inte övervägas inom ramen för utredningen.

En utökad möjlighet för myndigheter att fysiskt få tillgång till en viss handling som den individ som myndigheten möter innehar skulle kunna stärka kopplingen mellan etablerad identitet och verifiering av identitet, både genom en okulär kontroll mot ett fotografi på handlingen och med grund i biometriska uppgifter. Vi har i avsnitt 10.5.1 dock bedömt att det inte är möjligt eller lämpligt att lämna förslag om att tvångsåtgärder i form av exempelvis kroppsvisitation ska kunna vidtas av en bredare skara myndigheter, i ärenden av vitt skilda slag, för att kunna få tillgång till en handling. Tvångsåtgärder av det slag som i vissa situationer får vidtas med stöd av 9 kap. utlänningslagen – kroppsvisitation och undersökning av en utlännings bagage – utgör ett betydande ingrepp i rätten till skydd för privatlivet och måste där-

för motiveras av ett angeläget samhälleligt behov och stå i rimlig relation till det intresse åtgärden är avsedd att tillgodose.[34] Vidare kräver både biometrisk verifiering av identitet mot ett identitetsindex och mot en handling att biometriska underlag – i form av ansiktsbild och/eller fingeravtryck – kan tas upp. Att ge exempelvis Försäkringskassan eller en kommunal myndighet ett mandat att vidta tvångsåtgärder som kan innefatta ett mått av våld är emellertid helt uteslutet; de ärendeslag där sådana åtgärder får vidtas enligt gällande rätt är få och syftar i första hand till att upprätthålla en reglerad invandring och allmän ordning, vilket motiverar att tvångsåtgärder kan behöva vidtas. Detsamma kan enligt vår mening inte alls sägas för exempelvis ett ärende om en socialförsäkringsförmån eller ekonomiskt bistånd.

Mot denna bakgrund anser vi att det, inom ramen för utredningen, inte bör övervägas att ge myndigheter en möjlighet att vidta tvångsåtgärder i syfte att få till stånd en biometrisk verifiering av en persons identitet. Att det, enligt vår bedömning i avsnitt 18.3.2 och 20.3, inte bör regleras i författning hur biometriska underlag ska tas upp vid verifiering av identitet med hjälp av biometriska uppgifter, exempelvis genom ett krav på personliga inställelse, innebär givetvis inte att tvångsåtgärder får vidtas utan lagstöd för att sådana underlag ska kunna tas upp. I avsnitt 23.8 tar vi ställning till om bristande medverkan från den person vars identitet ska verifieras biometriskt ska kunna medföra någon konsekvens.

21.6 Verifiering med hjälp av en ansiktsbild mot ett identitetsindex

Vår bedömning

En myndighet bör få verifiera identitet genom kontroll mot ansiktsbild i ett identitetsindex i de situationer som anges i avsnitt 21.5, under förutsättning att identiteten i det enskilda fallet inte har kunnat verifieras biometriskt mot indexet.

För det fall en myndighets behov av att verifiera identitet med hjälp av biometriska uppgifter, mot ett identitetsindex, inte kan tillgodoses på detta sätt anser vi att det bör finnas möjlighet för myndigheten

[34] *Effektivare verktyg vid inre utlänningskontroll,* prop. 2023/24:12, s. 15.

att i stället verifiera identiteten med hjälp av den ansiktsbild som enligt vår bedömning bör lagras i ett sådant index. Det kan vara så att det i vissa fall inte är praktiskt möjligt att genomföra en biometrisk verifiering, till exempel för att den enskilde inte medverkar till att dennes ansiktsbild kan tas upp. Det kan också uppstå tekniska problem hos myndigheten i fråga eller vid själva kontrollen i systemet som förhindrar en biometrisk verifiering. För att myndighetens behov av verifiering – genom kontroll mot ett index – i dessa fall ändå ska kunna tillgodoses bör det vara möjligt att verifiera identitet genom kontroll mot en ansiktsbild, på det sätt vi beskrivit i avsnitt 18.4.

Verifiering med hjälp av ansiktsbild bör enligt vår mening endast vara ett andrahandsalternativ. En sådan metod för verifiering kräver visserligen inte behandling av biometriska uppgifter, vilket kan anses tala för att den bör få användas i första hand, eller i vart fall vara tillgänglig för myndigheten under samma förutsättningar som en biometrisk verifiering mot ett identitetsindex. En verifiering med hjälp av ansiktsbilden är dock inte lika säker som en biometrisk verifiering. I de fall myndigheten bedömer att det finns förutsättningar för och behov av en kontroll mot ett identitetsindex bör den därför i första hand göras i form av en biometrisk verifiering. En sådan verifiering bör – som vi beskrivit i avsnitt 21.5 – endast få genomföras i vissa situationer, nämligen om det är nödvändigt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde eller i annat fall om det är nödvändigt när en myndighet, inom ramen för sin verksamhet, genomför identitetskontroller. Med utgångspunkten att verifiering med hjälp av ansiktsbilden bör vara ett andrahandsalternativ ska denna metod endast få användas om dessa grundförutsättningar är uppfyllda. I enlighet med vad vi anfört ovan bör det vidare krävas att identiteten inte har kunnat verifieras genom kontroll mot biometriska uppgifter i ett identitetsindex. Anledningen till att verifieringen har misslyckats bör dock sakna betydelse.

Med tanke på det relativt begränsade intrång i den personliga integriteten som själva verifieringsprocessen innebär anser vi att det inte är oproportionerligt att biometrisk verifiering används i första hand när det är möjligt. Det är, enligt vår mening, inte heller oproportionerligt att möjliggöra att identitet verifieras med hjälp av ansiktsbild när biometrisk verifiering mot ett index inte är möjlig av någon anledning. Myndighetens behov av verifiering får anses väga tungt och den ansiktsbild som lämnats ut efter en begäran om verifiering bör

– som vi bedömt i avsnitt 18.5 – omedelbart förstöras efter att kontroll av identiteten har genomförts.

21.7 Förenlighet med dataskydd och grundläggande rättigheter

I avsnitt 5.2 har vi gett en översikt av dataskyddsförordningen och andra relevanta författningar på det dataskyddsrättsliga området och i avsnitt 5.3 har vi redogjort översiktligt för skyddet för den personliga integriteten i regeringsformen, Europakonventionen och EU:s rättighetsstadga. I kapitel 16 har vi tagit ställning till om den behandling av personuppgifter som behöver utföras i en verksamhet med ett identitetsindex uppfyller de grundläggande förutsättningarna enligt dataskyddsförordningen samt om de grundläggande förutsättningarna för inskränkning av rättigheter är uppfyllda. Vidare har vi i kapitel 17 bedömt att verksamheten med ett identitetsindex kan anses vara nödvändig och utgöra en proportionerlig inskränkning i skyddet för den personliga integriteten och privatlivet som följer av bestämmelser i regeringsformen, Europakonventionen och EU:s rättighetsstadga samt att verksamheten kan anses proportionerlig på det sätt som avses i artikel 9.2 g i dataskyddsförordningen. Vi underströk dock att det kan finnas utrymme för att göra en annan bedömning, såväl av lagstiftaren som av bland annat EU-domstolen, vilket vi återkommer till i avsnitt 22.11.

I det här avsnittet tar vi ställning till om användningen av en möjlighet att verifiera identitet biometriskt, antingen mot ett identitetsindex eller mot handlingar, kan anses förenlig med dataskyddsregelverket och grundläggande rättigheter. För att en myndighet ska kunna verifiera någons identitet biometriskt på dessa sätt är det nödvändigt att myndigheten behandlar personuppgifter. Den behandling som utförs måste då vila på en rättslig grund enligt artikel 6.1 e i dataskyddsförordningen (se avsnitt 5.2.3). Vid verifiering av identitet mot handlingar behöver myndigheten även behandla känsliga personuppgifter i form av biometriska uppgifter. Med hänsyn till vår bedömning i avsnitt 18.3.3 kommer det dock inte att vara nödvändigt för en myndighet som vill verifiera identitet genom kontroll mot ett identitetsindex att behandla biometriska uppgifter; då ska endast en ansiktsbild skickas in och de biometriska uppgifterna – som ska jämföras med

de biometriska uppgifter som tidigare lagrats i indexet – ska tas fram av systemet. Behandling av känsliga personuppgifter, vilket innefattar biometriska sådana, förutsätter att ett undantag i artikel 9.2 i dataskyddsförordningen är tillämpligt.

I avsnitt 21.7.1 belyser vi de rättsliga grunder enligt artikel 6.1 i dataskyddsförordningen som vi bedömer är aktuella vid biometriska kontroller av nämnda slag, nämligen allmänt intresse och myndighetsutövning. Vi tar i avsnitt 21.7.2 även ställning till de grundläggande krav som gäller för behandling av känsliga personuppgifter enligt artikel 9.2 i dataskyddsförordningen. I avsnitt 21.7.3 utvärderar vi om en möjlighet för en myndighet att verifiera identitet biometriskt i enlighet med våra överväganden i avsnitt 21.5 är proportionerlig och därmed förenlig med dataskyddsförordningen och grundläggande rättigheter.

21.7.1 Rättslig grund för att behandla personuppgifter

Vår bedömning

Nödvändig behandling av personuppgifter som utförs av en myndighet i syfte att biometriskt verifiera en persons identitet mot ett identitetsindex eller mot en handling kan utföras med stöd av de rättsliga grunderna *uppgift av allmänt intresse* och *myndighetsutövning* i artikel 6.1 e i dataskyddsförordningen.

För att personuppgiftsbehandling ska vara tillåten måste åtminstone ett av villkoren i artikel 6.1 i dataskyddsförordningen vara uppfyllt. Enligt vår mening finns tillämplig rättslig grund för personuppgiftsbehandling i samband med biometrisk verifiering av identitet mot antingen ett identitetsindex eller mot handlingar i första hand i artikel 6.1 e, det vill säga att behandlingen är nödvändig för att utföra en *uppgift av allmänt intresse* eller som ett led i *myndighetsutövning*. Av artikel 6.3 framgår att dessa grunder för behandlingen ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt, och att syftet med behandlingen ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Nämnda kriterier framgår även av 2 kap. 2 § dataskyddslagen (2018:218); i bestämmelsen specifi-

ceras när en uppgift av allmänt intresse eller myndighetsutövning ska utgöra rättslig grund för personuppgiftsbehandling enligt svensk rätt, i avsaknad av avvikande bestämmelser i annan författning.

Alla uppgifter som riksdag och regering har gett i uppdrag åt statliga myndigheter att utföra är av allmänt intresse i den mening som avses i dataskyddsförordningen. På motsvarande sätt är de uppgifter som ålagts kommuner och regioner att utföra av allmänt intresse (se avsnitt 5.2.3). Behandling av personuppgifter som en myndighet utför inom ramen för sin verksamhet för att kunna verifiera identitet för en person som myndigheten möter görs för att myndigheten ska kunna bedriva den verksamhet som faller inom ramen för dess befogenhet på ett korrekt, rättssäkert och effektivt sätt. Till detta kommer att den biometriska verifiering som vi i avsnitt 21.5 har bedömt att myndigheter bör få använda i vissa situationer syftar specifikt till att motverka identitetsmissbruk; EU-domstolen har i mål C-70/18, *Staatsecretaris van Justitie en Veiligheid mot A m.fl.,* bedömt att målet att förebygga och bekämpa identitets- och dokumentbedrägerier utgör tvingade skäl av allmänintresse. Vi anser mot denna bakgrund att den behandling av personuppgifter som en myndighet behöver utföra i samband med biometrisk verifiering av identitet mot ett identitetsindex eller mot en handling – i de situationer som anges i avsnitt 21.5 – är nödvändig av hänsyn till ett allmänt intresse. Behandlingen kan därför utföras med stöd av den rättsliga grunden *uppgift av allmänt intresse* i artikel 6.1 e i dataskyddsförordningen.

Enligt våra överväganden i avsnitt 21.5.1 bör biometrisk verifiering få användas i samband med handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Handläggningen av ett sådant ärende utmynnar normalt i ett bindande beslut av något slag, vilket utgör myndighetsutövning.[35] Kontroll av identitet, oavsett på vilket sätt det sker, utgör i sådana fall, som vi ser det ett led i handläggningen av ett ärende (jfr 19 § förvaltningslagen), och därmed myndighetsutövning. Om en myndighet utför nödvändig behandling av personuppgifter i syfte att biometriskt verifiera identitet mot ett identitetsindex eller mot en handling, som ett led i dess myndighetsutövning, bör även den rättsliga grunden *myndighetsutövning* i artikel 6.1 e i dataskyddsförordningen därför kunna tillämpas. När det gäller de situationer som avses i avsnitt 21.5.2 – nämligen när myn-

[35] *Om folkbokföring, samordningsnummer och identitetsnummer,* SOU 2021:57, s. 463.

digheten, inom ramen för sin verksamhet, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde genomför identitetskontroller – bör det, enligt vår bedömning, emellertid mer sällan vara fråga om myndighetsutövning. I sådana fall är det mer troligt fråga om så kallat faktiskt handlande, exempelvis i samband med att identitet kontrolleras vid inpassering till en myndighetslokal eller vid kontakt med en vårdinrättning.

När det gäller person- och samordningsnummer har dessa, som vi noterat i avsnitt 5.2.5, en särställning i dataskyddsförordningen. Enligt 3 kap. 10 § dataskyddslagen får sådana uppgifter behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Vi bedömer att behandlingen av person- och samordningsnummer vid biometrisk verifiering av identitet mot antingen ett identitetsindex eller mot handlingar – i de situationer som vi redogjort för i avsnitt 21.5 – är tillåten enligt 3 kap. 10 § dataskyddslagen, då den utförs dels av ett allmänt intresse, dels i syfte att möjliggöra en säker kontroll av identitet.

Mot bakgrund av det ovanstående bedömer vi att det finns en tillämplig rättslig grund för den behandling av personuppgifter som en myndighet kan komma att utföra vid en biometrisk verifiering mot antingen ett identitetsindex eller mot handlingar. Behandlingen är nödvändig för de syften som angetts ovan och den aktuella rättsliga grunden kommer – om en generell möjlighet till biometrisk verifiering införs – att vara fastställd i nationell rätt på det sätt som krävs enligt artikel 6.3 i dataskyddsförordningen. Detta då vi i avsnitt 21.2. har bedömt att en generell möjlighet för myndigheter att verifiera identitet biometriskt behöver regleras i lag.

21.7.2 Undantag för behandling av biometriska uppgifter

Vår bedömning

Nödvändig behandling av biometriska uppgifter vid verifiering av identitet mot ett identitetsindex eller mot en handling kan utföras med stöd av undantaget i artikel 9.2 g i förordningen, det vill säga ett *viktigt allmänt intresse*.

Som vi noterat inledningsvis i avsnitt 21.7 bör det, vid ett införande av ett system med ett identitetsindex, inte vara nödvändigt för en myndighet som vill verifiera identitet genom kontroll mot indexet att behandla biometriska uppgifter; endast de biometriska underlagen – som inte utgör känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen – behöver behandlas av en myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras. Om en myndighet däremot vill verifiera någons identitet biometriskt mot en handling kommer myndigheten att behöva utföra behandling av känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen. Även om behandlingen utförs lokalt i en applikation, exempelvis på den enskildes mobiltelefon eller i ett gemensamt backend-system (se avsnitt 27.4 för en teknisk beskrivning av hur detta kan genomföras), bedömer vi att den myndighet som bestämmer att verifieringen ska genomföras bör vara personuppgiftsansvarig för den behandling av känsliga personuppgifter som då utförs. Vi återkommer till frågan om personuppgiftsansvar i avsnitt 24.6.

Behandling av känsliga personuppgifter är enligt artikel 9.1 i dataskyddsförordningen som huvudregel förbjuden. I artikel 9.2 finns en uttömmande uppräkning av undantag, som ska tolkas restriktivt.[36] Det undantag som vi bedömer är relevant är det som framgår av artikel 9.2 g, nämligen behandling som är nödvändig med hänsyn till ett *viktigt allmänt intresse*, på grundval av unionsrätten eller medlemsstaternas nationella rätt, som ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga åtgärder för att kunna säkerställa den registrerades grundläggande rättigheter och intressen. Vi har i avsnitt 16.4.3 redogjort för de allmänna förutsättningarna för att tillämpa undantaget.

Det är som vi ser det givet att det utgör ett viktigt allmänt intresse att myndigheter – i de situationer vi redogjort för i avsnitt 21.5.1 och 21.5.2 – kan verifiera identitet på ett tillförlitligt sätt och med hjälp av biometriska uppgifter när detta är nödvändigt, oavsett om kontrollen görs mot uppgifter i ett identitetsindex eller i en handling. Verksamhet som innefattar myndighetsutövning anses generellt sett vara ett viktigt allmänt intresse. För myndigheters del innefattar detta bland annat den behandling av känsliga personuppgifter som är nödvändig för att de ska kunna utföra sina uppdrag enligt verksamhets-

[36] Se till exempel EU-domstolens dom i mål C-252/21, *Meta Platforms Inc*, punkt 76.

lagstiftning och respektive myndighets instruktion.[37] Vi bedömer att handläggning av ärenden som omfattas av förvaltningslagens tillämpningsområde alltid får anses falla inom en myndighets uppdrag, och normalt utgör myndighetsutövning. När det gäller biometrisk verifiering av identitet i sådana situationer som vi i avsnitt 21.5.2 bedömt också bör omfattas är det däremot sällan fråga om myndighetsutövning. Även i de fallen syftar verifieringen av identitet dock endast till att säkerställa om en person är den som han eller hon utger sig för att vara. En sådan säkrare identitetskontroll leder i det enskilda fallet till större upptäcktsrisk för personer som utger sig för att vara någon annan. Det kan få långtgående konsekvenser för den enskilde att få sin identitet utnyttjad, och att motverka detta syftar i förlängningen till att tillförsäkra enskilda ett godtagbart skydd för den personliga integriteten. EU-domstolen har i C-70/18, *Staatssecretaris van Justitie en Veiligheid mot A m.fl.*, bedömt att målet att förebygga och bekämpa identitets- och dokumentbedrägerier utgör tvingande skäl av allmänintresse (punkt 49). Att motverka identitetsmissbruk som möjliggör olika former av välfärdsbedrägerier eller andra typer av utnyttjande av identitet bör mot denna bakgrund också utgöra ett viktigt allmänt intresse i den mening som avses i artikel 9.2 g i dataskyddsförordningen.

Vi anser mot denna bakgrund att biometrisk verifiering av identitet, i de situationer som vi i avsnitt 21.5 bedömt att sådana kontroller bör få användas av myndigheter, alltid får anses ske av hänsyn till ett viktigt allmänt intresse. Den behandling som är nödvändig för att en myndighet ska kunna verifiera identitet under dessa förutsättningar har därmed stöd i undantaget i artikel 9.2 g i dataskyddsförordningen, under förutsättning att övriga villkor i bestämmelsen är uppfyllda.

[37] Prop. 2017/18:105, s. 83.

21.7.3 Proportionalitetsbedömning

Vår bedömning

Biometrisk verifiering av identitet mot ett identitetsindex eller en handling, i enlighet med våra bedömningar i avsnitt 21.5, utgör en proportionerlig inskränkning av skyddet för den personliga integriteten och privatlivet som följer av bestämmelserna i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Det är även proportionerligt på det sätt som avses i artikel 9.2 g i dataskyddsförordningen att behandla biometriska uppgifter vid sådan verifiering.

Frågan är hur den behandling av personuppgifter som utförs vid biometrisk verifiering mot ett identitetsindex eller en handling påverkar den personliga integriteten. Vi har i avsnitt 17.2 redogjort för utgångspunkter för den proportionalitetsbedömning som måste göras vid en inskränkning i skyddet av de rättigheter som framgår av regeringsformen, Europakonventionen och EU:s rättighetsstadga samt vid tillämpning av artikel 9.2 g i dataskyddsförordningen vid behandling av biometriska uppgifter. Med de utgångspunkterna gör vi följande bedömning.

Biometrisk verifiering av identitet medför ett visst intrång i den personliga integriteten …

Den behandling av personuppgifter som utförs vid en biometrisk verifiering av identitet påverkar enskildas personliga integritet. För det första behöver en ansiktsbild tas upp vid biometrisk verifiering mot såväl ett identitetsindex som mot en handling. Det kan under vissa omständigheter anses utgöra ett intrång i privatlivet i den mening som avses i artikel 8 i Europakonventionen och artikel 7 och 8 i EU:s rättighetsstadga att ta en ansiktsbild av en person utan hans eller hennes samtycke.[38] Det ska emellertid beaktas att själva upptagningen av det biometriska underlaget, det vill säga ansiktsbilden, inte anses innebära ett ingrepp i intimsfären och inte heller medför något större fysiskt eller psykiskt obehag för personen (EU-domstolens mål C-

[38] Prop. 2024/25:37, s. 47.

70/18, *Staatsecretaris van Justitie en Veiligheid mot A m.fl.*, punkt 58). Vid biometrisk verifiering mot en handling, i enlighet med våra överväganden i avsnitt 20.2, kan däremot även fingeravtryck komma att tas upp. Att ta någons fingeravtryck är ett sådant kroppsligt ingrepp som omfattas av skyddet i bestämmelsen i 2 kap. 6 § första stycket regeringsformen.

En myndighet som vill verifiera identitet biometriskt bör kunna begära att den enskilde låter myndigheten ta upp en ansiktsbild för att möjliggöra verifiering mot ett identitetsindex samt ta upp både ansiktsbild och fingeravtryck för att möjliggöra verifiering mot en handling. Myndigheten bör emellertid inte genom tvångsåtgärder kunna ta upp biometriska underlag för verifiering (se avsnitt 21.5.3). Den enskilde kan därmed motsätta sig att ansiktsbild eller fingeravtryck tas upp och på så sätt förhindra en behandling av sådana personuppgifter. Med hänsyn till att det finns en maktobalans mellan myndigheter och enskilda kan man dock tänka sig att den enskilde i många fall känner sig tvungen att på begäran från en myndighet medverka till att biometriska underlag kan tas upp och att det i praktiken inte finns någon direkt valfrihet. En möjlighet att förelägga den enskilde att medverka till kontrollen – eventuellt vid äventyr av att en framställan inte tas upp till prövning eller någon annan konsekvens – talar som vi ser det i samma riktning (se avsnitt 23.8). Det får således anses ske ett visst intrång i den personliga integriteten när biometriska underlag tas upp och detta särskilt när den enskilde egentligen motsätter sig biometrisk verifiering, men av någon anledning väljer att ändå medverka. Även framtagningen av biometriska uppgifter ur ansiktsbilden och fingeravtrycken och jämförelsen mot de biometriska uppgifter som antingen tidigare lagrats i ett identitetsindex eller tagits fram ur biometriska underlag i en handling i samband med kontrollen får anses medföra ett visst intrång i den personliga integriteten. Vid verifiering mot ett identitetsindex har vi bedömt att den myndighet som önskar verifiera identitet biometriskt inte ska ta fram biometriska uppgifter ur ansiktsbilden utan endast behandla ansiktsbilden (se avsnitt 18.3.3), vilket i viss mån begränsar det integritetsintrång som en verifieringsprocess kan innebära.

De övriga personuppgifter som kan behöva behandlas i samband med en biometrisk verifiering av identitet – det vill säga identitetsuppgifter och eventuellt identitetsbeteckning – innebär enligt vår mening inte något särskilt integritetsintrång. Det är för det första

fråga om mycket få personuppgifter som behandlas och uppgifterna kommer dessutom som utgångspunkt att ha lämnats av den enskilde i samband med att ärendet som föranleder verifieringen inleddes, eller i samband med en identitetskontroll i annat fall; behandlingen utförs endast i syfte att bekräfta att identitetsuppgifterna är korrekta. Omfattningen av behandlingen är vidare begränsad till en person vid verifiering med biometriska uppgifter eftersom det är fråga om en en-till-en-jämförelse. Någon möjlighet att ensidigt göra en sammanställning av uppgifter om flera individer finns inte, då biometrisk verifiering kräver medverkan av den enskilde vid verifieringstidpunkten vad gäller upptagning av biometriska underlag. Vid verifiering mot en handling krävs vidare att den enskilde gör handlingen i fråga tillgänglig. Ansiktsbild och/eller fingeravtryck som har tagits upp, samt de biometriska uppgifter som tagits fram ur dessa, i samband med verifieringen bör, enligt vår mening, dessutom förstöras direkt (se avsnitt 18.5 och 20.6). Med hänsyn till dessa omständigheter begränsas integritetsintrånget både vid verifiering mot ett identitetsindex och mot en handling.

Vid verifiering mot en handling blir det dessutom endast fråga om en momentan behandling av biometriska uppgifter, som inte ska få användas på något annat sätt, vid andra tillfällen eller utan den enskildes vetskap eller medverkan. Vidare har den enskilde – vid verifiering mot en handling – kontroll över det jämförelseunderlag, det vill säga handlingen, som används vid verifieringen. Därmed har den enskilde indirekt också kontroll över de biometriska uppgifter som tas fram och behandlas, vilket i sig begränsar i intrånget i den personliga integriteten.[39] Som framgår av avsnitt 21.5 är vår tanke också att möjligheten att verifiera identitet med hjälp av biometriska uppgifter ska användas endast när det är motiverat och vissa särskilda omständigheter är för handen.

Sammantaget anser vi att den behandling av personuppgifter som en myndighet kan komma att utföra i samband med en biometrisk verifiering av identitet mot ett identitetsindex eller mot en handling innebär ett visst intrång i den personliga integriteten enligt artikel 8 i Europakonventionen och artikel 7 och 8 i EU:s rättighetsstadga. Sådan behandling kan enligt vår mening emellertid inte anses utgöra ett betydande intrång i den personliga integriteten enligt 2 kap. 6 §

[39] EDPB:s yttrande den 23 maj 2024, *Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow*, s. 17.

andra stycket regeringsformen. Som vi påpekat ovan utgör det dock ett sådant kroppsligt ingrepp som omfattas av skyddet i bestämmelsen i 2 kap. 6 § första stycket regeringsformen att ta någons fingeravtryck, vilken enligt våra överväganden bör kunna aktualiseras vid biometrisk verifiering mot en handling.

… men motiveras av ett starkt allmänt intresse

Vid proportionalitetsbedömningen ska styrkan av det behov som ska tillgodoses genom inskränkningen i den personliga integriteten vägas mot inskränkningen. Syftet med att ge en bred krets av myndigheter möjlighet att kontrollera identitet biometriskt mot ett identitetsindex eller en handling är att motverka sådant identitetsmissbruk som vi redogjort för i kapitel 9. Detta syfte är som vi ser det av stor betydelse såväl för samhället som för enskilda. En utökad möjlighet till biometriska kontroller kompletterar, enligt vår mening, de möjligheter att genomföra identitetskontroller med grund i biometriska uppgifter vid etablering av identitet och vid utfärdande av identitetshandlingar som finns i dag, och som kommer att finnas vid genomförande av redan lämnade förslag. Att på detta sätt effektivt kunna kontrollera att en person är den som han eller hon utger sig för att vara samt motverka att personer som vistas i Sverige uppträder i olika identiteter i olika sammanhang är väsentligt för att kunna motverka identitetsmissbruk.

Ändamålet att minska möjligheten att använda till exempel kapade identiteter har i andra sammanhang, bland annat i fråga om mervärdesskattebedrägerier, ansetts anknyta till statens säkerhet, den allmänna säkerheten och förebyggande av oordning och brott och vara godtagbart i ett demokratiskt samhälle. I regeringens proposition *Åtgärder mot mervärdesskattebedrägerier* bedömdes att åtgärden att kontrollera biometriska uppgifter från såväl ansiktsbild som fingeravtryck i handlingar sammantaget inte bör anses gå utöver vad som är nödvändigt med hänsyn till ändamålet och därför inte står i strid med regeringsformen eller Europakonventionen.[40] Vi ser inte anledning att göra en annan bedömning i fråga om en möjlighet för myndigheter att – i enlighet med våra överväganden i avsnitt 21.5 – använda biometrisk verifiering av identitet vid såväl handläggningen av andra ärendeslag,

[40] Prop. 2025/26:128, s. 42.

exempelvis för att motverka felaktiga utbetalningar från välfärdssystemen, som när myndigheter i annat fall genomför identitetskontroller inom ramen för sin faktiska verksamhet.

Att samla in biometriska underlag och ta fram biometriska uppgifter i syfte att säkerställa korrekt identitet och minska risken för identitetsbedrägerier har även i lagstiftningsärenden på utlänningsrättens område ansetts syfta till att uppfylla viktiga allmänna intressen, och har inte bedömts utgöra ett otillbörligt intrång i den registrerades personliga integritet.41 Även EU-domstolen har uttalat sig angående begränsningar av de rättigheter som följer av artikel 7 och 8 i EU:s rättighetsstadga, i det ovan nämnda avgörandet, C-70/18, *Staatssecretaris van Justitie en Veiligheid mot A m.fl*. EU-domstolen konstaterade bland annat att förebyggande av identitetsbedrägerier utgör ett tvingande skäl av allmänt intresse. Vi kan här också notera att i förslaget till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem lyftes – i samband med överväganden om proportionalitet – fram bland annat att en korrekt verifiering av identiteten för en person kan anses ha en positiv inverkan på rätten till respekt för privatlivet, och i synnerhet rätten till en persons identitet, då detta kan bidra till mindre förvirring kring identiteten.[42] Vid en proportionalitetsbedömning bör därför beaktas att, utöver de kontrollmöjligheter som biometrisk verifiering mot ett index eller mot handlingar kan ge, medför sådan verifiering också ett skydd för enskilda mot att deras identitet utnyttjas av andra. Även målet att skydda enskilda är som vi ser det av stor betydelse från samhällssynpunkt.

Vid verifiering mot ett index bör de biometriska uppgifter som ska jämföras med sådana uppgifter i indexet, enligt vår bedömning, tas fram ur ansiktsbilden av systemet och inte av den myndighet som ska verifiera en persons identitet (se avsnitt 18.3.3). När en persons identitet verifieras biometriskt mot en handling bör det, enligt vår bedömning, i stället vara den myndighet som verifierar identitet som rättsligt ansvarar för behandlingen av de biometriska uppgifterna (se avsnitt 24.6). Vid biometrisk verifiering av identitet mot handlingar kommer behandlingen av biometriska uppgifter i rättslig bemärkelse alltså att utföras av en större krets av myndigheter än vid verifiering

[41] Se exempelvis prop. 2024/25:176, s. 39.
[42] Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration), COM(2017) 794 final, s. 18.

mot ett identitetsindex. Det medför, enligt vår bedömning, emellertid inte ett oproportionerligt intrång i skyddet för den personliga integriteten. Detta inte minst då myndigheterna – i vart fall i en sådan verifieringsprocess som beskrivs i avsnitt 27.4 – bör vara tekniskt förhindrade att ha tillgång till de biometriska underlagen och de biometriska uppgifter som kan tas fram ur dem.

I 3 kap. 3 § dataskyddslagen finns bestämmelser som kompletterar artikel 9.2 g i dataskyddsförordningen och reglerar när en myndighet får behandla känsliga personuppgifter med stöd av artikeln. Dataskyddslagen är enligt 1 kap. 6 § subsidiär och myndighets- eller verksamhetsspecifik reglering – såsom utlänningsdatalagen, domstolsdatalagen och ett sådant regelverk vi lämnar förslag om i kapitel 23 – har företräde. Regleringen är, enligt vår bedömning, ändå relevant eftersom den kan ge viss vägledning avseende under vilka förutsättningar det kan anses förenligt med artikel 9.2 g för en myndighet att behandla känsliga personuppgifter. Vi kan konstatera att enligt 3 kap. 3 § första stycket 2 dataskyddslagen får känsliga personuppgifter behandlas av en myndighet om behandlingen är nödvändig för handläggningen av ett ärende. Enligt vår bedömning är en möjlighet att verifiera identitet biometriskt vid handläggningen av ett ärende som omfattas av tillämpningsområdet för förvaltningslagen – i enlighet med våra överväganden i avsnitt 21.5.1 – förenlig med bestämmelsen, vilket med styrka talar för förenlighet även med dataskyddsförordningen.

Bestämmelsen i 3 kap. 3 § första stycket 3 dataskyddslagen tar i stället sikte på behandling av känsliga personuppgifter inom ramen för en myndighets faktiska verksamhet; regeringen bedömde att dataskyddslagen, mot bakgrund av vikten av att samhällets funktioner upprätthålls, bör ge myndigheter ett visst utrymme för behandling av känsliga personuppgifter även i den faktiska verksamheten.[43] Enligt bestämmelsen får känsliga personuppgifter behandlas om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Även här finns vissa likheter med en sådan möjlighet att verifiera en persons identitet biometriskt som vi övervägt i avsnitt 21.5.2, det vill säga när en myndighet i annat fall än vid handläggningen av ett ärende genomför identitetskontroller inom ramen för sin verksamhet. Att nödvändig behandling av biometriska uppgifter vid

[43] Prop. 2017/18:105, s. 88 ff.

verifiering av identitet kan utföras av hänsyn till ett viktigt allmänt intresse har vi redan bedömt i avsnitt 21.7.2. Vidare anser vi att en biometrisk verifiering inte kan anses innebära ett otillbörligt intrång i den enskildes integritet om verifieringen är nödvändig när en myndighet, inom ramen för sin verksamhet, genomför identitetskontroller. Myndighetens behov av säker verifiering av identitet får i en sådan situation anses stå i rimlig proportion till det relativt begränsade intrång i den personliga integriteten det innebär för den enskilde att identiteten verifieras på detta sätt. Detta får anses vara fallet både när kontrollen genomförs i myndighetens faktiska verksamhet och vid handläggningen av ett ärende eller mål som inte omfattas av förvaltningslagens tillämpningsområde.

Sammantaget är myndigheters behov av att kunna verifiera identitet på ett säkert sätt mycket stort och det samhällsintresse som ligger bakom detta behov är, enligt vår mening, angeläget. Med hänsyn till det, och till att det ingrepp i den personliga integriteten som en biometrisk verifiering i enlighet med våra överväganden medför får anses vara relativt begränsat, anser vi att åtgärden att kontrollera biometriska uppgifter från såväl ansiktsbild som fingeravtryck sammantaget inte kan anses gå utöver vad som är nödvändigt med hänsyn till ändamålet. I enlighet med vår bedömning i avsnitt 21.2 bör en rätt för myndigheter att kräva att den enskilde gör en viss handling tillgänglig för biometrisk kontroll, och i samband med detta låta myndigheten ta upp biometriska underlag, framgå av lag.

Vi anser mot denna bakgrund att biometrisk verifiering av identitet av aktuellt slag innebär en proportionerlig inskränkning i skyddet för den personliga integriteten och privatlivet som följer av bestämmelser i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Det är, enligt vår bedömning, även proportionerligt på det sätt som avses i artikel 9.2 g i dataskyddsförordningen att behandla biometriska uppgifter vid en sådan kontroll.

Det kan noteras att i det här avsnittet ligger fokus på den integritetspåverkan själva verifieringen innebär i det enskilda fallet, när en myndighet väljer att utnyttja möjligheten till biometrisk verifiering av identitet. Vi återkommer i avsnitt 22.11 till skillnaderna vad gäller påverkan på enskildas integritet mellan ett system med ett identitetsindex och ett system med utökad möjlighet att verifiera identitet biometrisk mot handlingar, där den största skillnaden, enligt vår bedömning, är att ett index kräver central lagring av biometriska upp-

gifter avseende alla personer vars identitet ska kunna verifieras med hjälp av indexet.

22 Jämförelse av de två huvudalternativen

22.1 Inledning

I kapitel 11–18 respektive 19–20 samt kapitel 21 har vi utrett två huvudalternativ för att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet för en bred krets av aktörer; biometrisk verifiering mot ett identitetsindex respektive mot handlingar. Vi har bland annat tagit ställning till när en person bör registreras i ett identitetsindex (se kapitel 13) och till vilka handlingar som är lämpliga att använda för en biometrisk verifiering (se kapitel 19), vilket påverkar den personkrets som kan kontrolleras med grund i biometriska uppgifter. Vi har också tagit ställning till vilka aktörer som bör kunna verifiera identitet genom kontroll mot ett identitetsindex respektive mot handlingar (se kapitel 21), vilket har betydelse för hur omfattande användningen av biometrisk verifiering kan antas bli, och därmed bland annat vilken effekt som kan antas uppnås.

I det här kapitlet jämför vi ett system med biometrisk verifiering mot ett identitetsindex med sådan verifiering mot handlingar i olika avseenden och redogör för relevanta skillnader som vi bedömer finns mellan de olika systemen, bland annat vilka personkategorier som kan fångas upp, omfattningen av intrånget i skyddet för den personliga integriteten samt komplexitet, såväl rättsligt som tekniskt. Vi avslutar kapitlet med en sammanställning av för- och nackdelar med de olika alternativen och vår bedömning av vilket alternativ som vi anser är att föredra.

22.2 Personkretsar som kan fångas upp

Utifrån våra överväganden i kapitel 13 om när en identitetsnyckel bör kunna skapas kan nedanstående slutsatser dras avseende den personkrets som skulle kunna verifieras biometriskt mot ett identitetsindex. De bedömningar vi gjort i kapitel 19 om vilka handlingar som är lämpliga för biometrisk verifiering ligger till grund för våra slutsatser avseende vilken personkrets som skulle kunna verifieras biometriskt mot handlingar.

22.2.1 Svenska medborgare

Svenska medborgare kommer primärt att kunna registreras i ett identitetsindex i samband med utfärdande av pass och statligt identitetskort och, under en övergångsperiod, den statliga e-legitimation som enligt föreslag i propositionen *En statlig e-legitimation* ska utfärdas enligt lag om statlig e-legitimation och elektronisk identifiering[1]. Enligt förslag i promemorian Ett statligt identitetskort ska den statliga e-legitimationen dock finnas på det statliga identitetskortet, när detta införs, och om den enskilde har en bärare av en statlig e-legitimation som utfärdats med stöd av lagen om statlig e-legitimation och elektronisk identifiering ska den makuleras innan ett statligt identitetskort lämnas ut.[2]

Vi bedömer att en mycket stor andel svenska medborgare kommer att välja att skaffa en eller flera av dessa handlingar regelbundet och att andelen är större för de svenska medborgare som bor i Sverige än de som bor utomlands. I undantagsfall kan en svensk medborgare komma att registreras i indexet i samband med inflyttning från utlandet eller tilldelning av samordningsnummer. Personer som blir svenska medborgare efter en anmälan eller ansökan om svenskt medborgarskap kommer att kunna registreras i ett index i samband med det, om de inte redan har registrerats i samband med till exempel utfärdande av uppehållstillståndskort. En stor majoritet av de svenska medborgarna kommer alltså, enligt vår bedömning, att kunna registreras i ett index, vilket innebär att deras identitet – som utgångspunkt – kommer att kunna verifieras biometriskt mot det.

[1] Prop. 2025/26:250, s. 5 ff.
[2] Ju2026/01595, s. 92 och 172.

Bedömningen att en mycket stor andel svenska medborgare kommer välja att skaffa en eller flera identitetshandlingar som utfärdas av svenska myndigheter innebär också att svenska medborgare – som utgångspunkt – kommer att kunna verifieras biometriskt med hjälp av sådana handlingar i stor utsträckning.

Sammanfattningsvis anser vi att möjligheterna att kunna verifiera svenska medborgares identitet biometriskt kommer att vara goda både med ett identitetsindex och vid verifiering mot handlingar.

22.2.2 EES-medborgare

Sannolikheten för att EES-medborgare som är folkbokförda i Sverige kommer att registreras i ett identitetsindex är, enligt vår bedömning, något lägre än för svenska medborgare och tredjelandsmedborgare som är folkbokförda. Vid utfärdande av pass och statligt identitetskort *ska* biometriska underlag tas upp. En folkbokförd EES-medborgare som ansöker om ett statligt identitetskort utan resefunktion kan därmed komma att registreras i ett index i samband med det. Det kan dock antas att det finns EES-medborgare som väljer att använda ett identitetskort från sitt hemland och inte ansöker om ett svenskt identitetskort. Även vid utfärdande av uppehållstillståndskort *ska* biometriska underlag tas upp; ett sådant kort utfärdas dock, som utgångspunkt, inte till EES-medborgare. Vid folkbokföring *kan* Skatteverket begära dels att den enskilde överlämnar en identitetshandling, dels att biometriska underlag tas upp för att kontrollera att dessa motsvarar dem som finns i handlingen. Det är således inte obligatoriskt med upptagning av biometriska underlag i ett ärende om inflyttning till Sverige. Eftersom den rättsliga möjligheten finns kan det i praktiken emellertid vara så att Skatteverket i mycket stor utsträckning genomför en biometrisk verifiering mot handlingar vid folkbokföring av EES-medborgare och att dessa då kan registreras i ett index.

EES-medborgare kan också komma att registreras i ett identitetsindex i samband med tilldelning av ett samordningsnummer. Här är förutsättningarna som utgångspunkt samma som vid folkbokföring; Skatteverket *kan* begära dels att den enskilde överlämnar en identitetshandling, dels att biometriska underlag tas upp för att kontrollera att dessa motsvarar dem som finns i handlingen. Folkbokföring kräver emellertid som huvudregel personlig inställelse, medan samordnings-

nummer på identitetsnivå sannolik och osäker kan tilldelas även om den enskilde inte inställer sig personligen.

Personer som tilldelats samordningsnummer utan att ha styrkt sin identitet – och som inte är svenska medborgare – kommer enligt lämnade förslag inte att kunna få ett statligt identitetskort.[3] Personer med samordningsnummer – som inte är svenska medborgare – kommer inte att kunna få en sådan statlig e-legitimation som ska utfärdas enligt förslag till lag om statlig e-legitimation och elektronisk identifiering, oavsett om identiteten har styrkts eller inte.[4] Endast vissa EES-medborgare som inte är folkbokförda kommer därmed – utifrån våra överväganden i kapitel 13 – att kunna registreras i indexet i samband med utfärdande av ett statligt identitetskort eller en sådan statlig e-legitimation.

Att EES-medborgare som vistas i Sverige i viss utsträckning avstår från att skaffa en svensk identitetshandling innebär inte att deras identitet inte kan verifieras biometriskt mot handlingar; även hemlandspass och identitetskort från andra länder som har utfärdats av behöriga myndigheter bör, enligt vår bedömning, som utgångspunkt kunna användas för en sådan kontroll (se avsnitt 19.3.1 och 19.3.2). EES-medborgare som vistas i Sverige kan på goda grunder antas ha antingen ett hemlandspass eller ett identitetskort, eller både och, eftersom det krävs för inresa i Sverige och nyttjande av den fria rörligheten inom EU. EES-medborgares identitet bör som utgångspunkt därmed gå att verifiera biometriskt mot handlingar.

22.2.3 Tredjelandsmedborgare

Tredjelandsmedborgare som folkbokförs i Sverige har i normalfallet beviljats uppehållstillstånd med en giltighetstid som överstiger ett år och ska då få ett uppehållstillståndskort utfärdat. I samband med utfärdande av kortet kan personen registreras i ett identitetsindex. Skatteverket kan också komma att ta upp biometriska underlag i samband med folkbokföring av en tredjelandsmedborgare, vilket möjliggör registrering av personen i ett index i samband med ett sådant ärende, om han eller hon inte redan är registrerad. De tredjelandsmedborgare som redan är folkbokförda när ett index tas i bruk

[3] Ju2026/01595, s. 7.
[4] Prop. 2025/26:250, s. 23.

kan antas kunna bli registrerade i ett index inom några år, i samband med utfärdande av ett uppehållstillståndskort, ett statligt identitetskort utan resefunktion eller en sådan statlig e-legitimation som ska utfärdas enligt lag om statlig e-legitimation och elektronisk identifiering.

Tredjelandsmedborgare som tilldelas ett samordningsnummer kan komma att registreras i ett identitetsindex i samband med det, under förutsättning att Skatteverket tar upp biometriska underlag vid den identitetskontroll som myndigheten ska göra vid tilldelningen. Upptagning av biometriska underlag förutsätter personlig inställelse, men samordningsnummer på identitetsnivå sannolik och osäker kan tilldelas även utan att personen i fråga inställer sig för identitetskontroll. Ett samordningsnummer kan alltså tilldelas utan att Skatteverket tar upp biometriska underlag. Personer med samordningsnummer på identitetsnivå sannolik och osäker – som inte är svenska medborgare – kommer, som vi nämnt i föregående avsnitt, inte att kunna få ett statligt identitetskort eller en sådan statlig e-legitimation som ska utfärdas enligt förslaget till lag om statlig e-legitimation och elektronisk identifiering. Dessa personer kommer därmed inte – utifrån våra överväganden i kapitel 13 – att kunna registreras i ett index i samband med utfärdande av en sådan handling.

Tredjelandsmedborgare med kortare uppehållstillstånd än ett år som varken folkbokförs eller tilldelas ett samordningsnummer kommer alltså inte att registreras i ett identitetsindex. Som vi bedömt i avsnitt 12.3.3 bör de som beviljats ett uppehållstillstånd som inte överstiger ett år emellertid inte enbart genom detta kunna antas få en sådan anknytning till Sverige att deras identitet kan behöva verifieras biometriskt mot ett identitetsindex.

Tredjelandsmedborgare, vars identitet kan antas komma att behöva verifieras, kommer sannolikt att vara innehavare av någon av de handlingar mot vilka en biometrisk verifiering, enligt vår bedömning i kapitel 19, bör kunna göras. Tredjelandsmedborgare som har beviljats uppehållstillstånd kommer att ha ett uppehållstillståndskort och den som vistas i Sverige med uppehållsrätt som familjemedlem till en EES-medborgare förutsätts ha ett giltigt hemlandspass, mot vilket en biometrisk verifiering kan göras, under förutsättning att handlingen innehåller ett digitalt lagringsmedium med biometriska underlag och identitetsuppgifter. Även andra tredjelandsmedborgare än familjemedlemmar till EES-medborgare kan – utöver uppehålls-

tillståndskortet – ha ett hemlandspass; merparten av de personer som beviljas uppehållstillstånd i Sverige har styrkt sin identitet med ett hemlandspass. Tredjelandsmedborgares identitet kommer därför normalt sett gå att verifiera biometriskt mot handlingar, om en sådan möjlighet införs.

22.3 Krav på medverkan

Registrering av en person i ett identitetsindex förutsätter endast indirekt medverkan av personen, eftersom registreringen sker i samband med handläggningen av ett ärende som denne initierat. Biometrisk verifiering mot ett identitetsindex kräver emellertid att den enskilde medverkar till upptagning av biometriska underlag, med hjälp av vilka en jämförelse kan göras mot de biometriska uppgifter som finns lagrade i indexet.

Också vid biometrisk verifiering av identitet mot handlingar är det en förutsättning att den vars identitet ska verifieras medverkar till att lämna biometriska underlag. Verifiering mot handlingar förutsätter också att personen i fråga är innehavare av en sådan handling mot vilken en kontroll bör kunna göras och gör den tillgänglig för den myndighet som ska verifiera identiteten. Handlingen utfärdas dock i ett tidigare skede, antingen efter ansökan av den enskilde om utfärdande av handlingen eller efter att den enskilde ansökt om och beviljats uppehållstillstånd och ett uppehållstillståndskort därmed utfärdats. Det är därför inte möjligt för myndigheten att veta anledningen till att den enskilde inte har någon handling tillgänglig som kan användas för verifiering och det är inte heller möjligt att tvinga den enskilde att skaffa en sådan handling.

Även om det, enligt vår bedömning, bör framgå av lag att det finns en skyldighet för den enskilde att låta en myndighet ta upp biometriska underlag samt – vid verifiering mot handlingar – göra en handling tillgänglig, kan det inte uteslutas att vissa personer kommer att motsätta sig att underlag tas upp eller inte kommer att göra en handling tillgänglig. Detta är som vi ser det en begränsning i båda system. Eventuella konsekvenser och åtgärder vid bristande medverkan från den enskilde, i ett system som bygger på verifiering mot handlingar, återkommer vi till i avsnitt 23.8.

22.4 Identifiering av okända personer

Identifiering av en person – på det sätt vi avser i det här betänkandet (se avsnitt 7.3.1) – kräver en sökning i ett register med hjälp av biometriska uppgifter, så kallad en-till-många-jämförelse. Som vi konstaterat tidigare är det inte möjligt att identifiera en person vid en sådan en-till-en-jämförelse som en biometrisk verifiering mot en handling innebär (se avsnitt 21.4). Vi har också tidigare bedömt att identifiering av en person i ett identitetsindex bör vara tillåten endast för att kunna avgöra om en identitetsnyckel ska skapas och att sådan identifiering bör göras av Skatteverket, Polismyndigheten och Migrationsverket (se avsnitt 18.2). Inget av de två huvudalternativ som jämförs i det här kapitlet kommer alltså att medföra möjlighet för fler aktörer än Skatteverket, Migrationsverket och Polismyndigheten att identifiera personer och dessa myndigheter kommer endast att kunna använda ett index för identifiering i ett mycket begränsat syfte. Information som kommer fram vid en identifiering i ett index kan dock vara användbar i till exempel Skatteverkets folkbokföringsverksamhet, om identifieringen visar att den enskilde registrerats med en annan identitet vid en tidigare kontakt med Skatteverket, Migrationsverket eller Polismyndigheten. Även om möjligheten att identifiera en person i ett index bör vara begränsad motverkar den etablering av multipla identiteter, vilket vi återkommer till i avsnitt 22.6.

22.5 Biometriska underlag som kan användas

Vi har tidigare bedömt att fingeravtryck och sådana biometriska uppgifter som kan tas fram ur dem inte bör lagras i ett identitetsindex (se avsnitt 11.4.5). Därmed kommer biometrisk verifiering mot ett index endast att kunna göras med en ansiktsbild och de biometriska uppgifter som tas fram ur bilden. Detta kan begränsa användningen i praktiken, exempelvis på grund av att viss teknisk utrustning inte fungerar vid ett visst verifieringstillfälle. Vad gäller biometrisk verifiering mot handlingar har vi däremot bedömt att såväl biometriska uppgifter som kan tas fram ur en ansiktsbild som ur fingeravtryck bör få användas för verifieringen (se avsnitt 20.2). Även en synlig ansiktsbild bör få användas (se avsnitt 20.2.4).

Vid verifiering mot en handling bör det ankomma på den myndighet som vill verifiera identiteten att avgöra vilka biometriska underlag

som tas upp och används i det enskilda fallet. Som vi lyft fram i sistnämnda avsnitt kan möjligheten för myndigheter att i praktiken använda biometriska underlag i form av fingeravtryck vid en verifiering mot en viss handling emellertid vara begränsad med hänsyn till tekniska skäl. En möjlighet att verifiera en persons identitet med hjälp av fingeravtryck kommer, enligt vår bedömning, vidare endast att kunna användas när personen i fråga inställer sig personligen hos myndigheten. Detta eftersom det med nuvarande tekniska lösningar inte är möjligt att ta upp biometriska underlag i form av fingeravtryck på distans (se avsnitt 20.2.3). Skillnaden i vilka biometriska underlag som bör kunna användas vid verifiering enligt de två huvudalternativen bör därmed inte få någon större betydelse i praktiken, innan relevant teknik har utvecklats ytterligare.

22.6 Möjlighet att motverka olika former av identitetsmissbruk

Både biometrisk verifiering mot ett identitetsindex och mot handlingar gör det möjligt att upptäcka om någon utger sig för att vara en annan person; verifieringen visar att personen i fråga inte är den person som registrerats med identiteten i ett index respektive inte är den person som den handling som personen använder för att legitimera sig har utfärdats för. Båda dessa sätt att verifiera identitet biometriskt kan därmed, enligt vår bedömning, motverka att identiteter utnyttjas eller kapas.

Biometrisk verifiering mot handlingar förhindrar dock inte att en person har handlingar i olika identiteter och uppträder i olika identiteter i olika sammanhang. De möjligheter Polismyndigheten, Skatteverket och Migrationsverket har – och vid genomförande av förslag som bereds inom Regeringskansliet kommer att ha – att verifiera personers identitet biometriskt vid utfärdande av olika rese- och identitetshandlingar kan dock antas kraftigt minska risken för att en person etablerar mer än en identitet i Sverige och därmed har handlingar som utfärdats av svenska myndigheter i flera olika identiteter.

Registrering av en person i ett index bör, enligt vår bedömning, ske i samband med handläggningen av ett ärende i vilket en så kallad grundidentitet etableras i Sverige eller en handling med identitetsuppgifter utfärdas av svenska myndigheter (se kapitel 13). Även om

identifiering av personer i ett identitetsindex endast bör få användas för att kunna avgöra om en identitetsnyckel ska skapas kommer en sådan identifiering att motverka dels att en person kan etablera flera identiteter i Sverige, dels att en person kan få handlingar utfärdade i olika identiteter av svenska myndigheter. En motsvarande möjlighet saknas i fråga om ett system som bygger på biometrisk verifiering av identitet mot handlingar.

Sammanfattningsvis kan biometrisk verifiering av identitet både mot ett identitetsindex och mot handlingar motverka att identiteter utnyttjas eller kapas, medan endast biometrisk verifiering mot ett identitetsindex direkt motverkar förekomst och användning av multipla identiteter.

22.7 Särskilt om kvalificerade skyddsidentiteter och personer med sekretessmarkering i folkbokföringen

Vi har tidigare bedömt att en identitetsnyckel bör kunna skapas i ett identitetsindex för en kvalificerad skyddsidentitet under vissa förutsättningar (se avsnitt 13.3.8). Ett system med ett identitetsindex bör, enligt vår bedömning, kunna utformas på ett sådant sätt att det är säkert även för personer med kvalificerade skyddsidentiteter. Detta med hänsyn till de begränsade möjligheter att identifiera en person som bör finnas och till att de beslutsmyndigheter som beslutar om kvalificerade skyddsidentiteter bör besluta om hur dessa ska hanteras i ett identitetsindex (se nämnda avsnitt). Under arbetets gång har dock både Polismyndigheten och Säkerhetspolisen framfört farhågor om att ett identitetsindex skulle medföra risker för personer med kvalificerade skyddsidentiteter. Av säkerhetsskäl har vi inte kunnat ta del av den information eller de underlag som ligger till grund för myndigheternas inställning. Det saknas emellertid anledning att ifrågasätta att det finns grund för myndigheternas synpunkter. Vi utgår därför från att ett system med ett identitetsindex medför vissa risker för personer med kvalificerad skyddsidentitet. En möjlighet att biometriskt verifiera identitet mot handlingar medför – såvitt kommit fram i utredningen – däremot inga särskilda risker för personer med kvalificerad skyddsidentitet. Personen i fråga agerar antingen privat, i den egna identiteten, eller i tjänsten, och kan då välja i vilken identi-

tet han eller hon agerar och vilken identitetshandling som ska göras tillgänglig för en myndighet, om personen har handlingar i flera olika identiteter.

Som vi lyft fram i avsnitt 11.4.6 och 13.2.2 behöver det – i ett system med ett identitetsindex – kontrolleras om en person som registreras i indexet har en sekretessmarkering i folkbokföringen. Det är av vikt att sådan information förs över till ett index, för att säkerställa att uppgifter som omfattas av en sekretessmarkering i folkbokföringen inte lämnas ut felaktigt. När information om sekretessmarkering för en individ ändras i folkbokföringen bör därför – i enlighet med våra bedömningar i avsnitt 14.3.3 – denna information uppdateras även i ett identitetsindex. Detta medför viss risk, även om det får förutsättas att rutiner införs som säkerställer att ändringar i folkbokföringen återspeglas i ett index. I ett system som bygger på biometrisk verifiering mot handlingar saknas helt sådana risker.

Mot denna bakgrund är en möjlighet att verifiera identitet mot handlingar att föredra från säkerhetssynpunkt – framför verifiering mot ett identitetsindex – för såväl personer med kvalificerad skyddsidentitet som personer som har en sekretessmarkering i folkbokföringen.

22.8 Olika aktörers möjlighet att verifiera identitet

Vi har tidigare bedömt att myndigheter bör få verifiera identitet biometriskt mot såväl ett identitetsindex som mot handlingar (se avsnitt 21.3.1). Med myndigheter avses i detta sammanhang samtliga statliga och kommunala organ, förutom riksdagen och de kommunala beslutande församlingarna. Alla organ som ingår i den offentligrättsliga statliga och kommunala organisationen bör alltså, som utgångspunkt, ha möjlighet att verifiera identitet biometriskt oavsett vilket av de två huvudalternativen som genomförs.

Vi har tidigare också bedömt att verifiering av identitet bör få genomföras under samma förutsättningar både vid verifiering mot ett index och mot handlingar, nämligen om det är nödvändigt vid handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde eller när en myndighet i annat fall, inom ramen för sin verksamhet, genomför identitetskontroller (se avsnitt 21.5). De rättsliga förutsättningarna för myndigheter kommer

alltså som utgångspunkt att vara samma med båda alternativen. Några omständigheter som inskränker de grundläggande förutsättningarna avseende i vilka situationer som myndigheter skulle kunna använda respektive system för biometrisk verifiering av identitet har vi inte identifierat. Som vi varit inne på ovan (se avsnitt 22.2) kommer det dock sannolikt att finnas vissa skillnader mellan alternativen i den personkrets vars identitet kan verifieras, vilket kan få betydelse för myndigheternas faktiska möjligheter att verifiera identitet biometriskt.

Enskilda aktörer kommer, i enlighet med vår tidigare bedömning (se avsnitt 21.3.2), varken att ha möjlighet att verifiera identitet mot ett identitetsindex eller mot handlingar. De huvudalternativ som utvärderas i detta och tidigare kapitel tar alltså båda primärt sikte på att motverka identitetsmissbruk som riktar sig mot offentliga aktörer.

22.9 Koppling till en grundidentitet

Registrering av personer i ett identitetsindex kommer att ske i samband med handläggningen av ett ärende i vilket en så kallad grundidentitet etableras i Sverige eller en handling med identitetsuppgifter utfärdas av en svensk myndighet (se kapitel 13). Om en person registreras i ett index i samband med etablering av personens identitet i Sverige blir kopplingen mellan identiteten och verifieringen av denna mot indexet givetvis stark; verifieringen bekräftar – eller utesluter – att personen som kontrolleras mot indexet också är den person som har etablerat den aktuella identiteten.

Vid utfärdande av en svensk identitetshandling – eller ett uppehållstillståndskort – handlar det snarare om att ge den enskilde en möjlighet att genom innehav av handlingen visa att han eller hon har en etablerad identitet i Sverige. Polismyndigheten och Migrationsverket har vissa – och har föreslagits få ytterligare – möjligheter att använda biometrisk verifiering vid utfärdande av sådana handlingar. Det medför att det vid utfärdandet av handlingen, och vid registreringen av en person i ett index i samband med utfärdandet, även finns en koppling till grundidentiteten. Den identifiering som, enligt vår bedömning i avsnitt 13.2.1, behöver göras mot ett index i samband med att en identitetsnyckel skapas inom ramen för ett ärende om utfärdande av relevanta handlingar innebär också att det efter att in-

dexet tagits i bruk inte kommer att vara möjligt för en person att få handlingar utfärdade av Polismyndigheten eller Migrationsverket i flera olika identiteter. Mot bakgrund av dessa omständigheter finns det vid verifiering mot ett index en stark koppling mellan en tidigare fastställd grundidentitet och verifiering av identiteten även när personen i fråga har registrerats i indexet i samband med utfärdande av en handling.

Hur stark kopplingen mellan en grundidentitet och verifiering av identiteten är vid biometrisk verifiering mot handlingar beror, enligt vår bedömning, i stor utsträckning på mot vilken typ av handling som verifieringen genomförs. Vid kontroll mot handlingar som utfärdats av svenska myndigheter finns det som vi ser det en stark sådan koppling; handlingen har utfärdats utifrån de identitetsuppgifter om personen i fråga som finns registrerade i Skatteverkets folkbokföringsverksamhet eller den centrala utlänningsdatabasen, och därmed i en etablerad identitet som personen har i Sverige. Vidare innehåller handlingarna vanligtvis en svensk identitetsbeteckning i form av personnummer eller samordningsnummer vilket gör det möjligt att enkelt koppla personen till den etablerade identiteten. Som vi noterat i avsnitt 19.3.3 innehåller ett uppehållstillståndskort inte Migrationsverkets individnummer. Det innebär som vi ser det emellertid inte att det saknas en koppling till den identitet som Migrationsverket har etablerat.

De svenska myndigheter som utfärdar identitetshandlingar och vissa andra handlingar med identitetsuppgifter har fått utökade möjligheter att verifiera identitet biometriskt inför utfärdandet, varför risken för att en person innehar svenska handlingar i flera identiteter har minskat. Det går emellertid inte att utesluta att en person har handlingar från svenska myndigheter i mer än en identitet. Det går som vi ser det inte heller att utesluta att en person innehar handlingar från sitt hemland i en identitet och handlingar från svenska myndigheter i en annan identitet.

Vid biometrisk verifiering mot handlingar som utfärdats av andra aktörer än svenska myndigheter är kopplingen mellan den i Sverige etablerade identiteten och verifiering av identiteten, enligt vår bedömning, betydligt svagare; innehållet i handlingen bygger inte på uppgifter om identitet som svenska myndigheter har tagit fram vid etableringen av en identitet, utan på uppgifter som utländska myndigheter har registrerat. Dessa kan bygga på ett oklart och icke tillförlitligt

underlag, beroende på landet i fråga. Ett utländskt pass innehåller visserligen uppgift om namn, födelsetid och medborgarskap – det vill säga om personens identitet – men identiteten behöver inte vara unik, och passet innehåller av förklarliga skäl varken en svensk identitetsbeteckning eller Migrationsverkets individnummer. Detsamma gäller för utländska identitetskort, som dessutom kan sakna uppgift om medborgarskap. Vi återkommer till detta i avsnitt 27.4.3, där vi bedömer att avsaknaden av en möjlighet att koppla en utländsk handling till en svensk identitetsbeteckning inte utgör en mer framträdande risk i praktiken. I det sammanhanget bedömer vi även att ett särskilt register för sådana kopplingar inte bör övervägas. Vid verifiering mot utländska handlingar kan det alltså komma att vara svårare att koppla personen och handlingen till en i Sverige etablerad grundidentitet.

Sammantaget bedömer vi att tillförlitligheten i en biometrisk verifiering mot ett identitetsindex i en del fall kan vara högre än tillförlitligheten vid sådan verifiering mot handlingar som inte har utfärdats av svenska myndigheter. Det beror på att kopplingen mellan en etablerad identitet och verifiering av identiteten är starkare vid en kontroll mot indexet än mot sådana handlingar. Med hänsyn till att det kan antas att den absoluta merparten av de som vistas i Sverige och vars identitet kan behöva verifieras biometriskt mot handlingar har tillgång till handlingar som utfärdats av svenska myndigheter – det vill säga ett svenskt pass, ett statligt identitetskort eller ett uppehållstillståndskort – saknas enligt vår mening dock någon avgörande skillnad i effektivitet, genomslag och tillförlitlighet för respektive system.

22.10 Rättslig och teknisk komplexitet

Skapandet av ett identitetsindex och införandet av en möjlighet att använda ett sådant index för biometrisk verifiering av identitet är, enligt vår bedömning, mycket komplext. Ett system med ett identitetsindex kräver tydliga rättsliga ramar vad gäller bland annat registrering av personer och löpande uppdatering av uppgifter i indexet samt användning av uppgifterna i indexet. Den omfattande centrala lagringen av biometriska uppgifter i systemet ställer mycket höga krav på innehållet i dessa rättsliga ramar för att säkerställa förenlighet med dataskyddsförordningen och grundläggande fri- och rättigheter. Regleringen behöver vara tydlig för myndigheter och enskilda och tillämp-

ningen förutsebar, vilket förutsätter ett relativt omfattande regelverk med i vissa avseenden detaljerade bestämmelser (se till exempel kapitel 13 och 14). Vidare kräver ett system med ett identitetsindex löpande åtgärder för att hålla uppgifterna i indexet uppdaterade och korrekta, och förutsätter samverkan mellan framför allt de tre myndigheter som enligt vår bedömning bör kunna skapa en identitetsnyckel samt registrera och uppdatera uppgifter i ett index, nämligen Skatteverket, Polismyndigheten och Migrationsverket. Även om personer bör kunna registreras i indexet och uppgifter uppdateras i detta i samband med handläggningen av vissa ärendeslag är det ändå inte fråga om att använda befintliga system och register, utan om att skapa ett helt nytt system för att möjliggöra biometrisk verifiering på ett säkert sätt. Det är av naturliga skäl en rättsligt och praktiskt mycket komplex och krävande process.

Även från teknisk synvinkel kan det med fog antas att ett system med ett identitetsindex innebär betydande komplexitet. Ett sådant system ställer synnerligen höga krav på tillgänglighet och kapacitet. De systemtekniska utmaningarna ligger inte bara i enskilda tekniska komponenter utan i kombinationen av beräkningsintensiv logik, hantering av en stor mängd uppgifter och en potentiellt mycket stor mängd samtidiga anrop med krav på snabba svarstider och hög driftsäkerhet. Ett identitetsindex utgör en enskild, systemkritisk felpunkt. När ett stort antal verifieringar behöver genomföras samtidigt uppstår snabbt processuella flaskhalsar, som belastar tillgängliga CPU/GPU-resurser[5] och minnesresurser. Belastningen ökar också på grund av den informationssäkerhet som ett index kräver, i form av kryptering och dekryptering av bland annat biometriska uppgifter i samband med en verifieringsbegäran. Även om ett index kan distribueras över ett flertal servrar eller datacenter kommer möjligheten att verifiera en person vid en given tidpunkt alltid att vara beroende av att systemet är tillgängligt och korrekt. Kommunikation mellan identitetsindexet och ett backend-system behöver även ske vid varje verifiering. Varje verifieringsbegäran måste snabbt och korrekt ledas till rätt nod i systemet, och en delning av information ställer också krav på replikering, så att uppdateringar av biometriska uppgifter och andra uppgifter som är kopplade till en identitetsnyckel slår igenom på ett korrekt sätt.

[5] CPU (Central Processing Unit) hanterar allmänna uppgifter och systemet med normalt få, kraftfulla kärnor, medan GPU (Graphics Processing Unit) kan ha tusentals mindre kärnor optimerade för att hantera många liknande uppgifter samtidigt (parallell bearbetning).

Sammantaget ställer detta krav på flera oberoende driftmiljöer som är geografiskt separerade samt att gemensamma felkällor – såsom delad nätverksinfrastruktur, delade åtkomstkedjor och delade administrationssystem – kan motverkas och i möjligaste mån elimineras. Betydande horisontell skalning, vilket är en metod inom databehandling där man ökar ett systems kapacitet genom att lägga till fler maskiner (servrar, instanser) i stället för att uppgradera en enskild maskin, kan antas vara nödvändigt. Att upprätthålla ett sådant system kräver en organisation och personal med särskild kompetens och erfarenhet av komplex, distribuerad drift. Ett identitetsindex måste också, med bibehållen drift, kunna uppgraderas och vidareutvecklas. Detta kan vara särskilt utmanande i en distribuerad miljö som alltid behöver vara i drift.

En möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar behöver givetvis också regleras rättsligt och även för detta alternativ är det viktigt med tydlighet och förutsebarhet, så att verifiering inte utförs i andra situationer än de som är tillåtna. Det är emellertid i huvudsak endast själva möjligheten att verifiera identitet som behöver regleras; det finns redan i dag tillämpliga regelverk för utfärdande av handlingar och personen vars identitet ska kontrolleras har med stor sannolikhet redan en identitetshandling eller ett uppehållstillståndskort. Efter att en biometrisk verifiering har genomförts bör dessutom både biometriska uppgifter och biometriska underlag förstöras (se avsnitt 20.6); inga sådana uppgifter bör få lagras av någon aktör efter genomförd kontroll och behöver inte heller lagras särskilt i ett tidigare skede för att möjliggöra verifieringen, till skillnad från vad som är fallet med ett identitetsindex. Någon uppdatering av uppgifter på det sätt som behöver kunna göras löpande i ett index är inte heller aktuellt. Det innebär att behovet av bestämmelser som reglerar behandlingen av personuppgifter, inklusive biometriska uppgifter, är betydligt mindre än med ett index. Det innebär också att tekniska system för biometrisk verifiering mot handlingar inte medför samma risker som ett identitetsindex, i vilket stora mängder känsliga personuppgifter lagras centralt.

Den tekniska infrastruktur som kan behövas för att implementera ett system baserat på biometrisk verifiering mot handlingar kan också antas vara mindre komplext än ett system som baseras på ett identitetsindex. I ett system som bygger på biometrisk verifiering mot en handling behöver de systemarkitektoniska utmaningarna inte samlas

till en central punkt på samma sätt som i ett identitetsindex utan kan fördelas mellan en mobilapplikation, som används för att ta upp biometriska underlag från den enskilde och från handlingens NFC-chip, och ett backend-system. Den biometriska jämförelsen skulle också potentiellt kunna genomföras helt i mobilapplikationen eller med användning av system som förvaltas av den myndighet som vill verifiera identitet. Det innebär att risken för en enskild, systemkritisk felpunkt – på det sätt som finns för ett system som bygger på ett centralt identitetsindex – minskar betydligt. Beroende på vilka logiska funktioner som placeras i mobilapplikationen respektive ett backend-system – vilket vi återkommer till i avsnitt 27.4 – kan systemresurskrävande behandling av information delas mellan mobilapplikationen och backend-systemet. Enligt vår bedömning kan behovet av en kraftfull, horisontellt skalbar och geografiskt distribuerad serverstruktur antas vara betydligt mindre i ett sådant system, oavsett om den biometriska jämförelsen genomförs i mobilapplikationen eller i ett backend-system. Viss horisontell skalbarhet förutsätts, men en betydande skillnad är att någon replikering av biometriska referensmallar över flertalet servrar och en betydande horisontell skalbarhet inte är tillämplig på samma sätt i ett system som bygger på verifiering mot handlingar. Någon uppdatering och replikering av identitetsuppgifter och biometriska uppgifter om en mycket stor mängd registrerade personer krävs inte, eftersom inga sådana uppgifter bör få sparas i samband med kontrollen mot en handling. Nödvändig redundans skulle i ett sådant system i stället till viss del kunna uppnås genom ett robust användarflöde i mobilapplikationen, med möjlighet att ta upp biometriska underlag på nytt om kvaliteten inte är tillräcklig för en jämförelse eller om backend-systemet tillfälligt inte skulle vara tillgängligt. En decentralisering av den biometriska jämförelseprocessen medför emellertid inte bara fördelar utan vissa systemarkitektoniska utmaningar, beroende på hur systemet utformas, vilket vi redogör för närmare i avsnitt 27.4. Även med hänsyn till detta bedömer vi att ett system med ett identitetsindex är betydligt mer komplext – både rättsligt och tekniskt – att införa, underhålla och använda än en möjlighet att verifiera identitet biometriskt mot handlingar.

22.11 Integritetspåverkan

Registrering i ett identitetsindex i samband med handläggningen av vissa ärendeslag innebär inte att biometriska underlag behöver tas upp särskilt för att en biometrisk verifiering senare ska vara möjlig; biometriska underlag hade – utifrån våra överväganden i kapitel 13 – ändå tagits upp av en myndighet. Biometriska underlag tas också upp i samband med utfärdande av de handlingar mot vilka en biometrisk verifiering bör kunna göras, oavsett om handlingen kommer att användas för sådan verifiering vid ett senare tillfälle. Den enskilde har i praktiken ingen möjlighet att motsätta sig upptagning av biometriska underlag varken i ett sådant ärende som ska kunna leda till registrering i indexet – inklusive utfärdande av vissa handlingar – eller vid utfärdande av en sådan handling mot vilken en biometrisk verifiering bör kunna göras; antingen ska myndigheten ta upp biometriska underlag eller så har myndigheten möjlighet att kräva att den enskilde lämnar sådana underlag. Vid utfärdande av en handling har den enskilde emellertid själv inlett ärendet, nämligen genom en ansökan om en viss handling eller om uppehållstillstånd. Upptagningen av underlag i sådana fall kan som vi ser det svårligen anses förenad med någon egentlig skyldighet eller någon typ av tvång.

Vid verifieringstillfället behöver biometriska underlag som huvudregel tas upp särskilt för att möjliggöra verifieringen. Det gäller både vid verifiering mot ett index och mot handlingar. I de fall verifieringen görs i ett sådant ärende som ska kunna leda till registrering eller uppdatering av uppgifter i ett index hade biometriska underlag emellertid tagits upp ändå. Vid verifiering mot ett index handlar det endast om att ta upp en ansiktsbild, medan det vid verifiering mot handlingar kan vara fråga om ansiktsbild, fingeravtryck eller både och. Det får anses utgöra ett större integritetsintrång att ta upp fingeravtryck än att ta upp en ansiktsbild.

Den största skillnaden mellan ett system med ett identitetsindex och en möjlighet att verifiera identitet biometriskt mot handlingar är, enligt vår bedömning, att det förstnämnda alternativet kräver central lagring av biometriska uppgifter avseende alla personer vars identitet ska kunna verifieras. Denna skillnad har stor betydelse för påverkan på enskildas personliga integritet. Registrering av ett mycket stort antal personer i ett identitetsindex och lagring av biometriska uppgifter avseende dessa innebär att även personer vars identitet aldrig

– eller sällan – kommer att verifieras biometriskt av en myndighet påverkas. Det kan alltså vara fråga om att uppgifter lagras för att de är ”bra att ha”, något som kan vara svårt att förena med principen om uppgiftsminimering i dataskyddsförordningen. Lagringen av biometriska uppgifter blir ett intrång även i dessa personers integritet.

Biometrisk verifiering mot handlingar kräver däremot endast att ytterligare behandling av personuppgifter utförs i samband med en faktisk verifieringssituation. En möjlighet att biometriskt verifiera identitet mot handlingar påverkar därmed endast de personer vars identitet kommer att kontrolleras på detta sätt av en myndighet, i de situationer vi redogjort för i avsnitt 21.5, vilket är en stor fördel från integritetssynpunkt. Vidare finns det, som vi ser det, en risk för att uppgifterna i ett identitetsindex – trots rättsliga och tekniska skyddsåtgärder – blir tillgängliga för obehöriga som kan använda uppgifterna i andra sammanhang, utan den enskildes kännedom eller samtycke. Vid biometrisk verifiering mot handlingar är det innehavaren av handlingen som förfogar över den och därmed över det biometriska jämförelseunderlag som används vid verifieringen. Det innebär, enligt vår bedömning, ett betydligt mindre integritetsintrång än verifiering mot ett index, och även en betydligt mindre risk för att känsliga uppgifter sprids till obehöriga. Att behandlingen av biometriska uppgifter, vid verifiering mot handlingar, i rättslig bemärkelse kommer att behöva utföras av en större krets av myndigheter leder enligt vår mening inte till någon annan bedömning. Detta då myndigheterna – i en sådan verifieringsprocess som beskrivs i avsnitt 27.3 och 27.4 – som utgångspunkt ska vara tekniskt förhindrade att ha tillgång till de biometriska underlagen och de biometriska uppgifter som kan tas fram ur dem; sådana uppgifter ska endast behandlas maskinellt, inte av någon handläggare hos myndigheten.

Vi har tidigare bedömt att både verksamheten med ett identitetsindex och en möjlighet att biometriskt verifiera identitet mot handlingar medför vissa inskränkningar i grundläggande rättigheter enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga (se kapitel 16, 17 och 21). Sådana inskränkningar kan emellertid vara tillåtna om de åtgärder som vidtas av det allmänna inte är mer ingripande än vad som är nödvändigt för att uppnå syftet med åtgärderna, det vill säga om de är proportionerliga. Myndigheters behandling av biometriska uppgifter av hänsyn till ett viktigt allmänt intresse, med stöd av artikel 9.2 g i dataskyddsförordningen, förutsätter också att

behandlingen står i proportion till det eftersträvade syftet (se avsnitt 16.4.3 och 21.7). Både ett system med ett identitetsindex och en möjlighet att biometriskt verifiera identitet mot handlingar förutsätter alltså proportionalitet för förenlighet med grundläggande rättigheter och med dataskyddsförordningen.

Med hänsyn till de skillnader från framför allt integritetssynpunkt som finns mellan dessa båda alternativ ser den proportionalitetsbedömning som behöver göras – och som vi har gjort tidigare i betänkandet – dock olika ut (se kapitel 17 och avsnitt 21.7.3). Biometrisk verifiering av identitet mot handlingar i de situationer då en sådan verifiering enligt vår bedömning bör vara möjlig har en relativt begränsad integritetspåverkan. Det kan, enligt vår mening, förhållandevis enkelt konstateras att det finns ett rimligt förhållande mellan det ingrepp i den enskildes rätt som en verifiering mot handlingar medför och det allmännas behov av att säkert kunna verifiera en persons identitet vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Detsamma får anses vara fallet när en biometrisk verifiering genomförs på grund av att en sådan kontroll är nödvändig när en myndighet i annat fall, inom ramen för sin verksamhet, genomför identitetskontroller. Proportionalitetsbedömningen avseende ett system med ett identitetsindex är däremot svårare och kräver mer ingående överväganden, särskilt vad gäller insamling och lagring av biometriska uppgifter i ett sådant centralt register.

Vi har tidigare bedömt att verksamheten med ett identitetsindex kan anses vara proportionerlig (se avsnitt 17.5). Det finns, enligt vår mening, dock ett större utrymme för att göra en annan bedömning än den vi gjort i frågan om proportionalitet vad gäller ett index än vad gäller en möjlighet att verifiera identitet biometriskt mot handlingar. Integritetsskyddsmyndigheten har under arbetets gång ifrågasatt proportionaliteten i att lagra biometriska uppgifter för en så omfattande personkrets som det är fråga om, och det finns omständigheter som enligt vår mening talar för att skapandet av ett identitetsindex innebär ett för stort ingrepp från det allmännas sida i förhållande till behovet av att motverka identitetsmissbruk, i synnerhet att även personer vars identitet aldrig eller sällan kommer att verifieras berörs genom att biometriska uppgifter kommer att lagras centralt också om dem. Även om det enligt vår mening är möjligt att vid en proportionalitetsbedömning landa i slutsatsen att ett identitetsindex står i proportion till det eftersträvade syftet går det, som vi ser det,

inte att med säkerhet konstatera att EU-domstolen skulle göra samma bedömning vid en eventuell framtida prövning. De integritetsrisker för enskilda som ett system med ett identitetsindex innebär medför, enligt vår bedömning, vissa risker för lagstiftaren, i det att det finns utrymme för olika bedömningar vad gäller frågan om proportionalitet. Det går som vi ser det därför inte att bortse från risken att möjligheten att implementera och använda ett sådant system begränsas eller helt uteblir. Motsvarande risk ser vi inte med ett system som bygger på en möjlighet för myndigheter att använda biometrisk verifiering mot handlingar; detta förekommer redan i många olika sammanhang, både nationellt och på unionsnivå.

22.12 Implementeringstid

Implementeringstiden kan, enligt vår bedömning, antas bli olika lång för ett system med ett identitetsindex respektive en möjlighet att biometriska verifiera identitet mot handlingar. Som vi varit inne på tidigare i det här kapitlet är ett identitetsindex mycket komplext både rättsligt och tekniskt och ett sådant system kräver mer omfattande förberedelser, bland annat för Skatteverket, Migrationsverket och Polismyndigheten. Dessutom kommer det att ta tid innan de personer som bör kunna verifieras biometriskt mot ett index har registrerats i detta; i avsnitt 13.3.2 och 13.3.3 har vi redogjort för med vilka intervall olika handlingar behöver förnyas, vilket har betydelse för när en majoritet av de personer som kan komma att omfattas av ett identitetsindex kommer att registreras, efter att indexet har tagits i drift. Möjligheterna att använda ett index för verifiering blir därmed begränsade inledningsvis.

Vid införande av en möjlighet att biometriskt verifiera identitet mot handlingar kan däremot alla personer som vid den tidpunkten har en relevant handling i princip kontrolleras direkt, i de situationer då förutsättningarna för verifiering är uppfyllda (se avsnitt 21.5). En möjlighet att verifiera identitet genom kontroll mot handlingar kräver vidare inte lika omfattande förberedelser, i form av framtagning av mer komplexa, nya, it-system och den hårdvara som krävs för att kunna bygga upp ett identitetsindex, och av arbetsrutiner hos berörda myndigheter. En sådan möjlighet bör därmed kunna införas snabbare. Oaktat att ny mjukvara i form av en sådan mobilapplika-

tion som vi beskriver i avsnitt 27.4 kan behöva utvecklas – om verifiering ska kunna genomföras på distans – är detta i sig inte en helt nödvändig förutsättning för att kunna biometriskt verifiera identitet mot handlingar; det bör som vi ser det kunna vara möjligt i vart fall för Polismyndigheten, Migrationsverket och Skatteverket att även utnyttja befintliga lösningar som redan i dag används för biometriska kontroller. Det kan även finnas möjlighet att genomföra biometrisk verifiering mot handlingar på plats vid något av Statens servicecenters kontor (jfr avsnitt 27.3 och avsnitt 25.2.1). En sådan lösning skulle kunna medföra en betydligt kortare implementeringstid, åtminstone för de myndigheter som är anslutna till Statens servicecenter, även om det kan kräva anpassning av befintliga system och avtal.

22.13 Kostnader

Det kan, enligt vår bedömning, med fog antas att ett system med ett identitetsindex medför högre kostnader för det allmänna än en möjlighet att biometriskt verifiera identitet mot handlingar. Pass, identitetskort och uppehållstillståndskort utfärdas löpande, oberoende av möjligheterna att kontrollera biometriska underlag på handlingarna. Det som framför allt behövs för att möjliggöra biometrisk verifiering mot handlingar är därmed system för verifiering, som varken ska innehålla biometriska uppgifter eller några andra personuppgifter utan bara möjliggöra momentana kontroller när förutsättningarna för biometrisk verifiering är uppfyllda. Det handlar alltså i detta avseende om tillfällig behandling av personuppgifter, som inte ska lagras särskilt av någon aktör med anledning av verifieringen. Det innebär att kostnaderna för det allmänna för att ta fram ett system för verifiering mot handlingar – vid jämförelse med ett system med ett identitetsindex – kan antas bli relativt begränsade, även om ett sådant system givetvis måste vara tillförlitligt, säkert och robust.

Att ta fram ett system för att möjliggöra biometrisk verifiering mot centralt lagrade uppgifter i ett identitetsindex är mer komplext och ställer högre krav på tillförlitlighet, säkerhet och robusthet. Redan skapandet av själva indexet kan antas medföra högre kostnader än att ta fram ett system för verifiering mot handlingar. Vidare behöver ett identitetsindex löpande tillföras uppgifter för att vara funktionellt, dels när personer registreras för första gången, dels när uppgifter om

tidigare registrerade personer uppdateras, vilket även det medför kostnader, bland annat genom att mer personal kan krävas för att genomföra dessa ytterligare moment. Förvaltningen av ett så omfattande och komplext system kan också antas medföra högre kostnader än förvaltningen av system som möjliggör biometrisk verifiering mot handlingar.

För de enskilda bör det inte bli någon skillnad kostnadsmässigt; varken verifiering mot ett index eller mot handlingar som genomförs av en myndighet bör medföra någon kostnad för den person vars identitet verifieras, utöver eventuella kostnader för resa och förlorad arbetsinkomst för det fall verifiering görs i samband med personlig inställelse, i det enskilda fallet (se avsnitt 30.3). Vid användning av ett system med verifiering mot handlingar kan man möjligen också tänka sig att den enskilde känner sig tvungen att skaffa en rese- eller identitetshandling, om han eller hon inte har en sådan handling mot vilken en verifiering bör få göras. Det kan dock antas höra till ovanligheterna att en person som vistas i Sverige och vars identitet en myndighet vill verifiera varken har pass, identitetskort eller uppehållstillståndskort.

Sammanfattningsvis bedömer vi att ett system med ett identitetsindex kan antas medföra betydligt högre kostnader för det allmänna än utökade möjligheter att biometriskt verifiera identitet mot handlingar. För enskilda bör det dock inte bli någon skillnad kostnadsmässigt mellan verifiering mot ett index respektive mot handlingar; det bör i normalfallet överhuvudtaget inte kosta den enskilde något att identiteten verifieras biometriskt.

22.14 Sammantagen bedömning

Vår genomgång i det här kapitlet visar att det finns ett flertal skillnader mellan de två huvudalternativ för att biometriskt verifiera identitet som vi har utvärderat. I tabellen nedan ges en översikt av de skillnader mellan ett system med ett identitetsindex och en möjlighet att verifiera identitet biometriskt mot handlingar som vi lyft fram ovan. Därefter redogör vi sammantaget för de för- och nackdelar med respektive alternativ som kommit fram samt avslutar med en bedömning av vilket alternativ som vi anser att utredningen bör gå vidare med.

Tabell 22.1 Skillnader mellan biometrisk verifiering av identitet mot ett identitetsindex och mot handlingar

Verifiering mot ett identitetsindex	Verifiering mot handlingar
Stark koppling till grundidentitet	Svagare koppling till grundidentitet för personer som saknar svenska handlingar
Hög tillförlitlighet	Lägre tillförlitlighet avseende personer som saknar svenska handlingar
Mycket omfattande, central, lagring och behandling av biometriska uppgifter	Ingen lagring av biometriska uppgifter
Kontroll av ansiktsbild	Kontroll av ansiktsbild eller fingeravtryck *alternativt* både ansiktsbild och fingeravtryck
Medverkan krävs vid verifierings-tillfället i form av upptagning av ansiktsbild	Medverkan krävs vid verifieringstillfället i form av tillgängliggörande av handling och upptag-ning av ansiktsbild och/eller fingeravtryck
Även personer som inte kontrolleras berörs	Endast personer som kontrolleras påverkas
Motverkar multipla, utnyttjade och kapade identiteter	Motverkar utnyttjade och kapade identiteter
Rättsligt och tekniskt komplext	Rättsligt och tekniskt enklare
Längre tid för implementering och uppbyggnadstid för indexet	Kortare implementeringstid och möjlighet till mer omedelbart genomslag
Relativt stora kostnader framför allt initialt, men också löpande	Lägre kostnader både initialt och över tid
Något mer begränsad personkrets	Mycket stor personkrets
Risker för personer med kvalificerad skyddsidentitet och sekretessmarkering i folkbokföringen	Ingen särskild risk för personer med kvalifi-cerad skyddsidentitet och sekretessmarkering i folkbokföringen

22.14.1 Ett system med ett identitetsindex

Ett system med ett identitetsindex förutsätter en mycket omfattande lagring av biometriska uppgifter och berör även personer vars identitet aldrig – eller sällan – kan antas komma att verifieras biometriskt. Dessa omständigheter medför en stor integritetspåverkan för en mycket stor personkrets, inklusive majoriteten av alla svenska medborgare. Integritetsskyddsmyndigheten har med hänsyn till detta varit skeptisk till ett identitetsindex under arbetets gång. Det finns, enligt vår mening, ett större utrymme för att göra en annan bedömning än den vi gjort i frågan om proportionalitet vad gäller ett index än vad gäller en möjlighet att verifiera identitet biometriskt mot handlingar. Det medför att det inte med säkerhet kan konstateras att ett system med ett identitetsindex, som utformas i enlighet med våra bedömningar i kapitel 11–18 och 21, skulle vara förenligt med data-

skyddsförordningen och grundläggande rättigheter. Med hänsyn till det innebär det, enligt vår bedömning, en risk för det allmänna att införa ett system med ett identitetsindex; systemet kan komma att underkännas av EU-domstolen vid en eventuell framtida prövning. Motsvarande risk föreligger – som vi bedömt i avsnitt 22.11 – inte i förhållande till ett system för biometrisk verifiering mot handlingar.

Ett system med ett identitetsindex är vidare både rättsligt och tekniskt mycket komplext att införa och kan som en följd av det, på goda grunder, antas medföra förhållandevis stora kostnader, både initialt för att ta fram it-system och löpande, till exempel för förvaltning av indexet. Även registrering och uppdatering av uppgifter i ett index som omfattar en stor del av befolkningen kan antas medföra behov av personal för i vart fall Polismyndigheten, Migrationsverket och Skatteverket, med de kostnader som detta innebär. Vi bedömer vidare att implementeringstiden för ett identitetsindex blir längre än för en möjlighet att verifiera identitet mot handlingar. Dessutom behöver ett index byggas upp innehållsmässigt efter att regelverket trätt i kraft, vilket kommer att ske i takt med att Skatteverket, Polismyndigheten och Migrationsverket handlägger aktuella ärendeslag. Det kan därmed ta några år.

Ett system med ett identitetsindex har fördelen att det kan motverka etablering och användning av multipla identiteter på ett annat mer direkt sätt än verifiering mot handlingar och vi bedömer att den starka kopplingen till grundidentitet som följer av verifiering mot ett index ger en något högre tillförlitlighet i verifieringen än verifiering mot handlingar, i vart fall handlingar som är utfärdade av utländska myndigheter. Ett identitetsindex kan därför, enligt vår mening, vara ett mer effektivt verktyg för att motverka olika former av identitetsmissbruk än en möjlighet att verifiera identitet mot handlingar. Med hänsyn till att vårt huvuduppdrag är att stärka verifiering av etablerade identiteter och till att risken för utnyttjade och kapade identiteter bedöms vara mer omfattande än renodlat falska identiteter anser vi dock att dessa omständigheter inte uppväger de ovan anförda nackdelarna med ett identitetsindex. Det bör också beaktas att ett identitetsindex endast möjliggör biometrisk verifiering av de personer som har registrerats i indexet, medan möjligheten att biometriskt verifiera identitet mot handlingar potentiellt omfattar alla som har en relevant handling.

En annan omständighet att ta hänsyn till vid ställningstagande till vilket av huvudalternativen som utredningen bör gå vidare med är att Polismyndigheten under arbetets gång har motsatt sig ett system med ett identitetsindex. Polismyndigheten har i stället förespråkat en lösning som bygger på redan befintliga nationella och EU-gemensamma informationssystem, vilket vi har tagit ställning till i avsnitt 10.6. Vidare har Polismyndigheten framfört att de utmaningar som finns inom identitetsförvaltningens område främst är kopplade till personer som inte är svenska medborgare; av våra direktiv följer dock att målsättningen med ett system för säkrare verifiering av identitet bör vara att så många som möjligt som vistas i Sverige på sikt ska kunna ingå. Polismyndigheten är emellertid en mycket central myndighet vad gäller den statliga identitetsförvaltningen och skulle, enligt vår bedömning, vara helt central för ett system med ett identitetsindex; införande av ett sådant system förutsätter i stor utsträckning Polismyndighetens medverkan. Myndighetens framförda inställning till ett identitetsindex riskerar som vi ser det att försvåra – och i praktiken eventuellt även hindra – genomförande av ett förslag om införande av ett system med ett sådant index.

22.14.2 Biometrisk verifiering av identitet mot handlingar

En stor fördel med biometrisk verifiering mot handlingar är att en sådan möjlighet inte kräver central lagring av biometriska uppgifter och därmed att endast de personer vars identitet kontrolleras på detta sätt kommer att påverkas direkt. Det gör integritetsintrånget betydligt mindre än det intrång som ett identitetsindex medför. Utfallet av den proportionalitetsbedömning som behöver göras för att ta ställning till förenlighet med dataskyddsförordningen och grundläggande rättigheter är, enligt vår bedömning, inte heller osäkert, på det sätt motsvarande bedömning för ett system med ett index kan vara. En möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar kan, som vi ser det, inte anses vara mer ingripande än vad som är nödvändigt för att uppnå syftet att motverka användning av utnyttjade och kapade identiteter vid kontakt med offentliga aktörer. Det får anses gälla både vid verifiering som är nödvändig vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde och vid verifiering som är nödvändig när en

myndighet, i annat fall, genomför identitetskontroller inom ramen för sin verksamhet. Vi har svårt att se att EU-domstolen, vid en eventuell prövning, på ett generellt plan skulle motsätta sig ett regelverk som ger myndigheter en möjlighet att verifiera identitet biometriskt mot handlingar, särskilt med hänsyn till att biometrisk verifiering mot handlingar redan är en central del i många EU-gemensamma förordningar, i vart fall på utlänningsrättens område. Det kan också nämnas att EU-kommissionen har lämnat förslag till ändringar i artikel 9.2 i dataskyddsförordningen, bland annat att ett nytt led ska läggas till; ”*Behandlingen av biometriska uppgifter är nödvändig för att bekräfta en registrerad persons identitet (kontroll), om den registrerade har ensam kontroll över de biometriska uppgifter eller de medel som krävs för kontrollen*”.[6]

Vidare bedömer vi att verifiering mot handlingar utgör ett rättsligt och tekniskt sett enklare alternativ än ett identitetsindex, som dessutom kräver kortare implementeringstid än ett index och i princip kan få ett omedelbart genomslag. Kostnaderna kan också antas vara betydligt lägre både initialt och sett över tid, än för ett index.

En möjlighet att verifiera identitet biometriskt mot handlingar motverkar – till skillnad från ett identitetsindex – emellertid inte etablering och användning av multipla identiteter. Vidare blir kopplingen till en i Sverige etablerad grundidentitet för vissa personkategorier något svagare, vilket i sin tur ger en något lägre tillförlitlighet i verifieringen av dessa personer än verifiering mot ett index. En möjlighet att verifiera identitet mot handlingar kan med hänsyn till dessa omständigheter vara mindre effektivt för att motverka olika former av identitetsmissbruk än ett index. En sådan möjlighet tar dock sikte på säkrare verifiering av etablerade identiteter, vilket är fokus för vårt uppdrag. Med hänsyn till de möjligheter att kontrollera identitet biometriskt som Polismyndigheten, Skatteverket och Migrationsverket har – och kommer att ha vid genomförande av förslag som bereds inom Regeringskansliet – finns det dessutom goda möjlighet framöver att motverka att identitetshandlingar och uppehållstillståndskort utfärdas i flera olika identiteter för en och samma person. Detta ökar tillförlitligheten i en verifiering mot handlingar och innebär att olika delar av identitetsförvaltningen kan komplettera varandra. Som vi påpekat ovan omfattar en möjlighet att verifiera identitet biometriskt mot handlingar potentiellt alla som har en relevant handling, vilket

[6] Se COM(2025) 837 final, 2025-11-19.

enligt vår bedömning ger en större personkrets än vid verifiering mot ett index.

22.14.3 Sammanfattande slutsats

Vår bedömning

Ett system för säkrare verifiering av identitet med grund i biometriska uppgifter bör bygga på en möjlighet för fler myndigheter att kontrollera sådana uppgifter mot handlingar.

Mot bakgrund av genomgången i det här kapitlet anser vi att fördelarna med ett identitetsindex inte är av sådant slag att de väger upp nackdelarna. Ett system med ett identitetsindex bör, enligt vår mening, alltså inte föreslås av utredningen. Vi bedömer att en möjlighet att biometrisk verifiera identitet mot handlingar med god verkan kan förhindra att utnyttjade och kapade identiteter används vid kontakter med myndigheter. Med hänsyn till att en sådan möjlighet medför ett betydligt mindre integritetsintrång för enskilda än ett system med ett identitetsindex och kan antas vara mer kostnadseffektiv, anser vi att ett system för säkrare verifiering av identitet, med grund i biometriska uppgifter, bör bygga på en möjlighet för fler myndigheter att kontrollera sådana uppgifter mot handlingar. I kapitel 23–29 redogör vi för de särskilda frågor – om bland annat dataskydd och sekretess samt tekniska lösningar och informations- och cybersäkerhet – som aktualiseras i ett sådant system, och lämnar de författningsförslag som behövs.

Statens offentliga utredningar 2026

Kronologisk förteckning

1. Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. Fi.
2. 710 miljoner skäl till reformer. Ju.
3. Genomförande av plattformsdirektivet. A.
4. Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. U.
5. Utvidgad avdragsrätt för sponsring m.m. Fi.
6. En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. S.
7. Förstärkt uppföljning och utvärdering av folkhälsopolitiken.
   Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser.
   Del II: Utvärdering av alkoholpolitikens styrmedel. S.
8. Rättssäker samhällsvård för barn och unga. S.
9. Registrering av EES-medborgare. Ju.
10. Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. Ju.
11. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
12. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
13. Straffansvar för deltagande i och samröre med kriminella sammanslutningar. Ju.
14. Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. KN.
15. Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. Ku.
16. Försvarsexportinitiativ. För gemensam säkerhet. Fö.
17. Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. LI.
18. Odlingstorv och klimatet. Fi.
19. Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. S.
20. Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. Fi.
21. Återkallelse av svenskt medborgarskap. Ju.
22. Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. S.
23. Tolkavgift och förbud mot barntolkning. A.
24. Mervärdesskatt vid uthyrning och överlåtelse av fastighet. Fi.
25. Ett smittskydd för framtiden. S.
26. Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. Ju.
27. Lättnader i kraven på hållbarhetsrapportering. Ju.
28. Tillgång till passageraruppgifter i brottsbekämpningen. Ju.
29. Förbud mot uppfödning av djur för pälsproduktion. LI.
30. Mer flexibla regler om verkställighet av häktning och fängelsestraff. Ju.
31. Ett investeringsprogram för kultur. Ku.
32. Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. KN.
33. Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. KN.

34. Nya nätbrott och andra åtgärder för genomförandet av direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Volym 1 & 2. Ju.
35. En åldersgräns för barns tillgång till sociala medier. S.
36. Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. S.
37. Förutsättningar för en likvärdig och språkutvecklande förskola. U.
38. Behovsstyrd vård. S.
39. Ett nytt system för återkrav inom socialförsäkringen. S.
40. Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. KN.
41. Jämställdhet i en föränderlig tid – nuläge och vägar framåt. Volym 1 & 2. A.
42. Ett nytt regelverk för granskning av utländsk finansiering av trossamfund och andra verksamheter. Volym 1 och 2. Ju.
43. Åtgärder mot överskuldsättning. Fi.
44. En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning. Fi.
45. Effektiva ingripanden mot brott i cybermiljö. Ju.
46. Ett sammanhållet, robust och konkurrenskraftigt Sverige – framtidens politik för utveckling i landsbygder och regioner. LI.
47. Rätt till ersättning vid avveckling av kärnkraft på grund av politiska beslut – reaktorer som inte tagits i drift. KN.
48. Tillträdesförbud. Ju.
49. Traditionell eller rationell. En premiepension som kan nå målen. S.
50. En ny speciallärarutbildning. U.
51. Fri att lära och leva. Insatser mot hedersrelaterat våld och förtryck i förskolan, skolan och fritidshemmet. U.
52. En reform av den statliga barn- och ungdomsvården. Volym 1, 2 och 3. S.
53. Parallella samhällsstrukturer – ett kunskapsunderlag för förbättrad integration och minskat utanförskap. A.
54. Stärkt egendomsskydd i regeringsformen. Ju.
55. Säkrare verifiering av identitet. Volym 1 och 2. Fi.

Statens offentliga utredningar 2026

Systematisk förteckning

Arbetsmarknadsdepartementet

Genomförande av plattformsdirektivet. [3]

Tolkavgift och förbud mot barntolkning. [23]

Jämställdhet i en föränderlig tid – nuläge och vägar framåt. Volym 1 & 2. [41]

Parallella samhällsstrukturer – ett kunskapsunderlag för förbättrad integration och minskat utanförskap. [53]

Finansdepartementet

Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. [1]

Utvidgad avdragsrätt för sponsring m.m. [5]

Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. [11]

Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. [12]

Odlingstorv och klimatet. [18]

Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. [20]

Mervärdesskatt vid uthyrning och överlåtelse av fastighet. [24]

Åtgärder mot överskuldsättning. [43]

En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning. [44]

Säkrare verifiering av identitet. Volym 1 och 2. [55]

Försvarsdepartementet

Försvarsexportinitiativ. För gemensam säkerhet. [16]

Justitiedepartementet

710 miljoner skäl till reformer. [2]

Registrering av EES-medborgare. [9]

Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. [10]

Straffansvar för deltagande i och samröre med kriminella sammanslutningar. [13]

Återkallelse av svenskt medborgarskap. [21]

Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. [26]

Lättnader i kraven på hållbarhetsrapportering. [27]

Tillgång till passageraruppgifter i brottsbekämpningen. [28]

Mer flexibla regler om verkställighet av häktning och fängelsestraff. [30]

Nya nätbrott och andra åtgärder för genomförandet av direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Volym 1 & 2. [34]

Ett nytt regelverk för granskning av utländsk finansiering av trossamfund och andra verksamheter. Volym 1 och 2. [42]

Effektiva ingripanden mot brott i cybermiljö. [45]

Tillträdesförbud. [48]

Stärkt egendomsskydd i regeringsformen. [54]

Klimat- och näringslivsdepartementet

Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. [14]

Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. [32]

Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. [33]

Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. [40]

Rätt till ersättning vid avveckling av kärnkraft på grund av politiska beslut – reaktorer som inte tagits i drift. [47]

Kulturdepartementet

Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. [15]

Ett investeringsprogram för kultur. [31]

Landsbygds- och infrastrukturdepartementet

Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. [17]

Förbud mot uppfödning av djur för pälsproduktion. [29]

Ett sammanhållet, robust och konkurrenskraftigt Sverige – framtidens politik för utveckling i landsbygder och regioner. [46]

Socialdepartementet

En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. [6]

Förstärkt uppföljning och utvärdering av folkhälsopolitiken. Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser. Del II: Utvärdering av alkoholpolitikens styrmedel. [7]

Rättssäker samhällsvård för barn och unga. [8]

Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. [19]

Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. [22]

Ett smittskydd för framtiden. [25]

En åldersgräns för barns tillgång till sociala medier. [35]

Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. [36]

Behovsstyrd vård. [38]

Ett nytt system för återkrav inom socialförsäkringen. [39]

Traditionell eller rationell. En premiepension som kan nå målen. [49]

En reform av den statliga barn- och ungdomsvården. Volym 1, 2 och 3. [52]

Utbildningsdepartementet

Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. [4]

Förutsättningar för en likvärdig och språkutvecklande förskola. [37]

En ny speciallärarutbildning. [50]

Fri att lära och leva. Insatser mot hedersrelaterat våld och förtryck i förskolan, skolan och fritidshemmet. [51]