Skyddet för den personliga integriteten

Kartläggning och analys

Del 1

Delbetänkande av Integritetsskyddskommittén

Stockholm 2007

STATENS OFFENTLIGA UTREDNINGAR

SOU 2007:22

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar
av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av
Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.
Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Textbearbetning och layout har utförts av Regeringskansliet, FA/kommittéservice

Tryckt av Edita Sverige AB
Stockholm 2007

ISBN 978-91-38-22724-4
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet Beatrice Ask

Regeringen bemyndigade den 7 april 2004 chefen för Justitiedepartementet att tillkalla en kommitté (Ju 2004:05) med högst elva ledamöter med uppdrag att bl.a. kartlägga och analysera sådan lagstiftning som rör den personliga integriteten samt överväga dels om 2 kap. 3 § andra stycket regeringsformen bör ändras, dels om det vid sidan av befintlig lagstiftning behövs generellt tillämpliga bestämmelser till skydd för den personliga integriteten. Rättschefen Olle Abrahamsson förordnades den 13 maj 2004 att vara ordförande i kommittén. Till ledamöter i kommittén förordnades den 27 augusti 2004 riksdagsledamöterna Inger Davidson, Christer Engelhardt, Liselott Hagberg, Inger René och Alice Åström samt dåvarande riksdagsledamöterna Anders Bengtsson, Leif Björnlod, Agne Hansson, Barbro Hietala Nordlund och Ulla Wester. Inger Davidson entledigades den 4 oktober 2004 och samma dag förordnades dåvarande riksdagsledamoten Olle Sandahl att som ledamot ingå i kommittén. Den 23 oktober 2006 entledigades Barbro Hietala Nordlund som ledamot i kommittén med verkan fr.o.m. den 1 november 2006.

Den 18 januari 2007 beslutade regeringen med ändring av det tidigare beslutet att kommittén skall bestå av högst tolv ledamöter, varefter riksdagsledamöterna Bertil Kjellberg och Annie Johansson den 22 januari 2007 förordnades till ledamöter i kommittén.

Kommittén antog namnet Integritetsskyddskommittén.

Till experter förordnades den 9 september 2004 kanslirådet Katrin Hollunger Wågnert, byråchefen Daniel Kjellgren och chefsjuristen Leif Lindgren.

Som sekreterare i kommittén anställdes den 16 augusti 2004 kammarrättsassessorn Elisabet Reimers och den 1 april 2006 hovrättsassessorn Märit Bergendahl.

Kommittén överlämnar härmed delbetänkandet *Skyddet för den personliga integriteten – kartläggning och analys.*

Kommittén fortsätter nu sitt arbete med överväganden rörande behovet av ny lagstiftning till skydd för den personliga integriteten.

Stockholm den 29 mars 2007

Olle Abrahamsson

Anders Bengtsson

Christer Engelhardt

Agne Hansson

Bertil Kjellberg

Olle Sandahl

Alice Åström

Leif Björnlod

Liselott Hagberg

Annie Johansson

Inger René

Ulla Wester

/
Elisabet Reimers

Märit Bergendahl

Innehåll

Del 2

Regelverket

Bilagor

Förkortningar

a. a.	anfört arbete
a. prop.	anförd proposition
a. st.	anfört stycke
AD	Arbetsdomstolen
AFL	lagen (1962:381) om allmän försäkring
AMV	Arbetsmarknadsverket
ASP	Allmänna spaningsregistret
bet.	betänkande
BrB	brottsbalken
BRU	Beredningen för rättsväsendets utveckling
CSN	Centrala studiestödsnämnden
dir.	direktiv
dnr	diarienummer
Ds	Departementsserien
EG	Europeiska gemenskapen/gemenskaperna
EpC	Epidemiologiskt Centrum
EU	Europeiska unionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Europa-konventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
f.	följande sida/sidor
FPL	förvaltningsprocesslagen (1971:291)
FB	föräldrabalken
FL	förvaltningslagen (1986:223)
FN	Förenta Nationerna
FRA	Försvarets radioanstalt
FT	Förvaltningsrättslig tidskrift
FUN	Försvarets underrättelsenämnd
HSL	Hälso- och sjukvårdslagen (1982:763)

HSAN	Hälso- och sjukvårdens ansvarsnämnd
IS UNDSÄK	Informationssystemet för den militära underrättelse- och säkerhetstjänsten
IUP	individuell utvecklingsplan
JK	Justitiekanslern
JO	Riksdagens ombudsmän
JT	Juridisk Tidskrift vid Stockholms universitet
KFMdbL	lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet
KSI	Kontoret för särskild inhämtning
LEK	lagen (2003:389) om elektronisk kommunikation
LPK	lagen (1998:506) om punktskattekontroll av transporter m.m. av alkoholvaror, tobaksvaror och mineraloljeprodukter
LPT	lagen (1991:1128) om psykiatrisk tvångsvård
LRV	lagen (1991:1129) om rättspsykiatrisk vård
LSS	lagen (1993:387) om stöd och service till vissa funktionshindrade
LSU	lagen (1998:603) om verkställighet av sluten ungdomsvård
LVM	lagen (1988:870) om vård av missbrukare i vissa fall
LVU	lagen (1990:52) med särskilda bestämmelser om vård av unga
LYHS	lagen (1998:531) om yrkesverksamhet på hälso- och sjukvårdens område
MUC	Centrum för maritima underrättelser
MUST	Militära underrättelse- och säkerhetstjänsten
NJA	Nytt juridiskt arkiv, avdelning 1
OSEK	Offentlighets- och sekretesskommittén
PO	Allmänhetens pressombudsman
PON	Pressens opinionsnämnd
PPM	Premiepensionsmyndigheten
prop.	proposition
PuL	personuppgiftslagen (1998:204)
RF	regeringsformen
RB	rättegångsbalken
RÅ	Regeringsrättens årsbok
SBE	skattebrottsenhet
SCB	Statistiska centralbyrån
SekrL	sekretesslagen (1980:100)

SFS	Svensk författningssamling
SiS	Statens institutionsstyrelse
SIS	Schengens informationssystem
SkadestL	skadeståndslagen (1972:207)
skr.	regeringens skrivelse
SofdL	lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration
SofdF	förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration
SoL	socialtjänstlagen (2001:453)
SoLPuL	lagen (2001:454) om behandling av personuppgifter inom socialtjänsten
SoLPuLF	förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten
SOU	Statens offentliga utredningar
SPAR	Statens personadressregister
SvJT	Svensk Juristtidning
SÖ	Sveriges internationella överenskommelser
TF	tryckfrihetsförordningen
UB	utsökningsbalken
UF	utsökningsförordningen (1981:981)
YGL	yttrandefrihetsgrundlagen

Sammanfattning

Detta delbetänkande innehåller en bred kartläggning och analys av sådan lagstiftning som rör den personliga integriteten men däremot inga lagförslag eller överväganden rörande någon ny generell reglering på området. I ett tjugotal på varandra följande avsnitt sammanfattas i förevarande volym regelverket på olika områden (en mer fullständig redogörelse finns i betänkandets andra del). I anslutning till vart och ett av dessa avsnitt redovisar kommittén sin bedömning av rättsläget utifrån ett integritetsskyddsperspektiv. De samlade bedömningarna jämte kommitténs övergripande slutsatser återfinns sedan i kapitel 24 *Sammanfattande analys*. Det kapitlet innesluter följaktligen essensen av kommitténs arbetsresultat och utgör i sig en sammanfattning av betänkandets innehåll.

Så som betänkandet således är strukturerat har kommittén inte funnit det påkallat att utarbeta en sammanfattning av traditionellt slag; en sådan skulle i huvudsak endast komma att upprepa innehållet i kapitel 24 *Sammanfattande analys*. Den följande redogörelsen är därför tämligen kortfattad och har delvis karaktär av en utvidgad och kommenterad innehållsförteckning.

Kapitel 1 Utredningsuppdraget

I kapitlet redogörs för kommitténs direktiv och för betänkandets disposition samt för hur utredningsarbetet har bedrivits.

Kapitel 2 Utgångspunkter och avgränsningar

Här beskrivs översiktligt de internationella konventioner och svenska grundlagsbestämmelser som syftar till att ge skydd åt den enskildes integritet. Dessa grundläggande regler kommer kommittén senare att behandla mer utförligt i sitt slutbetänkande.

I kapitlet undersöks också hur begreppet personlig integritet har definierats i olika sammanhang samt anges en praktiskt fungerande metod för att avgränsa det skyddsvärda område som kommittén har i uppgift att kartlägga och analysera. Avgränsningen bör enligt kommittén ta sin utgångspunkt i informationen om den enskilde och inkludera användningen av identifieringsdata. Det konstateras att en sådan avgränsningsmetod fångar in de mest skyddsvärda inre skikten av den personliga integriteten och är väl lämpad att ligga till grund för kartläggningsarbetet.

Vidare ges en översikt över den tekniska utvecklingen som har betydelse för integritetsskyddet. Inte bara dagens teknik beskrivs utan också en tänkbar framtida utveckling. Två aktuella utvecklingslinjer anges: En där syftet direkt är att åstadkomma ökad kontroll, spårbarhet och övervakning av individer samt en annan där tekniken i sig är harmlös men där dess tillämpning kan förorsaka integritetsskadliga sidoeffekter.

Kapitel 3 Kommitténs attitydundersökning i sammandrag

Kapitlet sammanfattar resultatet av en attitydundersökning som kommittén låtit utföra i samarbete med Statistiska centralbyrån. Syftet med undersökningen har varit att få en ungefärlig uppfattning om allmänhetens inställning till behovet av skydd för den personliga integriteten, särskilt när detta behov kommer i konflikt med andra berättigade intressen. Drygt 1 000 slumpvis utvalda personer besvarade ett 80-tal frågor på en rad olika områden av betydelse för integritetsskyddet. Undersökningen, som torde vara den första i sitt slag som inte har varit avgränsad till en viss fråga eller till någon särskild aspekt på integritetsskyddet, redovisas i sin helhet i en bilaga till betänkandet.

Kapitel 4 Generella skyddsregler i vanlig lag

I detta kapitel redogörs för regler i vanlig lag som syftar till att skydda den personliga integriteten i mer generell bemärkelse och alltså inte endast inom ett visst område. Hit hör i främsta rummet brottsbalkens bestämmelser om fridsbrott, ärekränkning och brott mot tystnadsplikt samt vissa bestämmelser som kan grunda rätt till skadestånd vid kränkningar av den personliga integriteten. Kapitlet

avslutas med en relativt utförlig genomgång av generellt tillämpliga EG-rättsliga respektive svenska bestämmelser om skydd för personuppgifter i samband med framför allt automatiserad databehandling.

Redovisningen av de generella skyddsreglerna i detta kapitel utgör en nödvändig bakgrund till de särskilda skyddsregler som finns på de olika specifika rättsområdena. Någon analys av i vad mån det generellt gällande integritetsskyddet är tillfredsställande reglerat görs dock inte i detta sammanhang, utan är en uppgift som kommittén återkommer till i sitt slutbetänkande.

Kapitel 5 Skatteområdet

Kommittén konstaterar bland annat att det inte har lämnats någon godtagbar förklaring till varför möjligheterna att på skatteområdet lämna ut uppgifter till andra myndigheter är mycket större än på andra områden där absolut sekretess gäller. Vidare har bestämmelserna om att skattebrottsenheterna inom Skatteverket skall ha direktåtkomst i beskattningsdatabasen införts utan en tillräcklig redovisning och analys av behovet och av konsekvenserna för integritetsskyddet. Den avvägning mellan behovet av effektivitet och behovet av integritetsskydd som finns redovisad i lagmotiven är, delvis som en konsekvens av den bristfälliga behovsanalysen, inte heller tillräcklig.

Kapitel 6 Exekutionsväsendet

År 2001 infördes i lagstiftningen en förstärkt sekretess på kronofogdemyndigheternas område. Ett bakomliggande syfte var att få till stånd ett effektivare informationsutbyte mellan kronofogdemyndigheterna och andra myndigheter. Tanken var att om sekretessen hos kronofogdemyndigheterna stärktes skulle andra myndigheter i ökad utsträckning kunna lämna känslig information vidare till kronofogdemyndigheterna. I lagstiftningsärendet redovisades inte i vad mån det kunde finnas andra, för integritetsskyddet mindre ingripande, möjligheter för kronofogdemyndigheterna att använda sig av enligt sekretesslagstiftningen för att uppnå det önskade effektivitetsmålet. Kommittén konstaterar att det av den anledningen saknas underlag för att kunna bedöma hur nöd-

vändig lagändringen var. Inte heller redovisades det vilka konsekvenser som kunde förväntas från integritetsskyddssynpunkt av ett ökat informationsflöde mellan olika myndigheter.

Vidare anmärker kommittén att bestämmelserna om behandling av personuppgifter som tar sikte på eller får återverkningar på frågan om utlämnande av uppgifter från Kronofogdemyndigheten, har utformats utan att det tydliggjorts hur bestämmelserna förhåller sig till regler om sekretess. En förstärkning av integritetsskyddet har däremot blivit följden av att det införts sekretess för enstaka skuldbelopp.

Kapitel 7 Kreditupplysning och inkasso

På området för kreditupplysning och inkasso anser kommittén att det från integritetsskyddssynpunkt är olyckligt att skyddet för den enskildes integritet, som annars följer av framför allt kreditupplysningslagen, inte kan upprätthållas vid kreditupplysning via Internet eller andra elektroniska kommunikationstjänster. Förhållandet utnyttjas av bland andra företag som erbjuder kreditupplysning via SMS-meddelanden och en webbplats. Dessa företag kan utan risk för påföljd underlåta att iaktta kravet på att lämna en kreditupplysningskopia till den som avses med upplysningen och har heller ingen skyldighet att rätta oriktiga eller missvisande uppgifter. Grundorsaken till problemet är att det år 2003 infördes vissa grundlagsändringar som syftade till att stärka skyddet för yttrandefriheten. De risker som ändringarna förde med sig för den personliga integriteten uppmärksammades alltför litet i lagstiftningsärendet.

Kapitel 8 Domstolarna

De regler som på domstolsområdet berör integritetsskyddet grundas på sedan lång tid vedertagna värderingar. Reglerna innebär att intresset av offentlig insyn i många fall ges företräde framför enskildas intresse av skydd för den personliga integriteten. Emellertid konstaterar kommittén att de frågor om sekretess som uppkommer i samband med olika handläggningsåtgärder ofta är relativt komplicerade samt att det i stor utsträckning har överlämnats till domstolen själv att ta ställning till dessa frågor. Som såväl JO som

JK påtalat förekommer det också felaktigheter vid domstolarnas handläggning av hithörande frågor. Mot den bakgrunden ifrågasätter kommittén om inte mer resurser, främst i form av utbildningsinsatser, bör avsättas till domstolarnas handläggning av sekretessfrågor.

Kommittén framhåller också att det inte är tillfredsställande att domstolarnas behandling av personuppgifter ännu inte har blivit föremål för annat än en provisorisk lagreglering.

Kapitel 9 Straffprocessuella tvångsmedel

Genom lagstiftning år 2004 fick polisen ökade möjligheter att använda hemliga tvångsmedel. Det skedde genom att andra principer antogs än de som lagstiftaren tidigare under lång tid hade sagt vara grundläggande från rättssäkerhets- och integritetsskyddssynpunkt. Såvitt framgår av lagmotiven genomfördes reformen utan att nya eller tidigare okända omständigheter åberopades och utan att de negativa effekterna för den enskildes integritetsskydd analyserades så ingående som man hade kunnat förvänta sig vid en så stor förändring. Någon bedömning av om det polisiära behovet av ändringarna stod i proportion till de åtföljande försämringarna i integritetsskyddet, redovisades heller inte i lagstiftningsärendet, vilket särskilt mot bakgrund av frågans betydelse måste betraktas som en brist.

Kommittén konstaterar vidare att den parlamentariska kontrollen över tvångsmedelsanvändningen är svag och i praktiken inskränkt till jämförelser mellan andelen resultatrika tvångsmedelsanvändningar från ett år till ett annat. Den årliga redovisningen till riksdagen baseras i stort sett enbart på uppgifter från Åklagarmyndigheten och Rikspolisstyrelsen. Dessa uppgifter sätts inte i relation till andra relevanta uppgifter. På senare år har en kraftig ökning skett av antalet meddelade tillstånd till användning av tvångsmedel. Vad denna ökning beror på går inte att avläsa i de lämnade redovisningarna. Årsvisa fluktuationer i antalet meddelade tillstånd och i antalet resultatrika fall kommenteras inte närmare. Inte heller redovisas bakgrundsmaterial och jämförande material. Åtskilliga anmärkningar av systemkaraktär kan alltså riktas mot det sätt varpå den parlamentariska kontrollen över tvångsmedelsanvändningen bedrivs. Trots att bristerna har varit kända under lång tid har ingen ny ordning för insyn och kontroll införts.

Det nyligen införda systemet med offentliga ombud utgör enligt kommitténs mening ett välkommet initiativ från statsmakternas sida, inte minst mot bakgrund av den ökade risk för integritetsförluster som 2004 års reform innebär. Det är emellertid svårt att bedöma i vad mån ordningen med offentliga ombud har fyllt sitt syfte, eftersom det ännu inte gjorts en noggrann uppföljning och utvärdering av hur väl ordningen har fungerat.

I kapitlet redogör kommittén också för de i riksdagen vilande regeringsförslagen om hemlig rumsavlyssning (s.k. buggning) och om åtgärder för att förhindra vissa särskilt allvarliga brott (användande av tvångsmedel i preventivt syfte). Kommittén tar i sak inte ställning vare sig för eller emot förslagen men riktar kritik mot det sätt varpå förslagen har tagits fram och presenterats. Särskilt gäller detta beskrivningen av förslagens integritetsskadliga effekter, som kommittén finner vara otillräcklig, samt tillämpningen av proportionalitetsprincipen. Kommittén tar också de båda lagstiftningsärendena som utgångspunkt för ett antal reflektioner av mer allmän karaktär när det gäller integritetsskyddet i lagstiftningen.

Kapitel 10 Polisens spaningsmetoder

För att kunna fullgöra sina uppgifter är polisen beroende av spaningsmetoder som innebär någon form av avlyssning eller övervakning och som många gånger sker i hemlighet. Vissa metoder förutsätter att tekniska hjälpmedel används, såsom handmanövrerade kameror, dolda kroppsmikrofoner, inspelningsapparatur och pejlingsutrustning. Metoderna ger i stor utsträckning upphov till kränkningar av enskildas personliga integritet. Även om lagenligheten av en del av dessa metoder genom åren har ifrågasatts från olika håll, kan bedömningen inte göras att polisen bör avstå från att i nuvarande omfattning använda de aktuella metoderna på grund av att de alltför mycket inkräktar på den personliga integriteten. Däremot är det önskvärt att integritetskänsliga spaningsmetoder blir föremål för reglering. Det oreglerade tillstånd som nu råder synes medföra betydande risker för att det lokalt eller på individnivå föranstaltas om spaningsmetoder som inte tillräckligt beaktar integritetsskyddsintresset. Först genom en reglering blir det möjligt att generellt dra rågången mellan tillåtna och icke tillåtna metoder samt ta ställning till andra frågor av betydelse för

integritetsskyddet, såsom vem som skall ha behörighet att besluta om teknisk spaning och vilka kompensatoriska skyddsåtgärder som behövs.

Kapitel 11 Sekretess och behandling av personuppgifter i polisens verksamhet

Behovet av en ny polisregisterlagstiftning har länge varit känt. Redan år 1999 bedömde regeringen att det av hänsyn till integritetsskyddet var viktigt med en översyn av reglerna om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det måste emellertid konstateras att detta översynsarbete ännu inte har lett till någon ny lagstiftning. Förhållandet är desto mer beklagligt som polisen under senare år har fått tillgång till en allt större mängd integritetskänslig information och även med tanke på det omfattande och energiska reformarbete som samtidigt ägt rum i syfte att ge polisen effektivare metoder att hämta in information både för spaning och brottsutredning. De faror för den personliga integriteten som följt med dessa ökade polisiära befogenheter har alltså inte kompenserats genom stramare och säkrare personregisterregler. Kommittén gör bedömningen att det uteblivna reformarbetet på detta område inte är acceptabelt från integritetsskyddssynpunkt.

Nyligen fick polisen väsentligt utvidgade möjligheter att registrera uppgifter från DNA-analyser. Allmänt sett kan det förefalla som om de integritetsförluster som lagändringen innebar, uppvägs av de starkt förbättrade möjligheterna att klara upp brott. Emellertid hade regering tidigare avvisat en så långtgående registreringsmöjlighet som infördes genom reformen. Skälet till att denna mer restriktiva inställning frångicks framgår inte av lagmotiven, vilket gör det svårt att bedöma om behovet av lagändringen stod i proportion till dess negativa inverkan på integritetsskyddet.

Kapitel 12 Den civila säkerhetstjänsten (Säkerhetspolisen)

Säkerhetstjänstkommissionen uttalade år 2002 skarp kritik både mot den lagstiftning som reglerar tvångsmedelsanvändningen inom Säkerhetspolisen och mot det sätt varpå denna lagstiftning tilläm-

pas. Kommissionens kritik har emellertid ännu inte föranlett någon ny ordning för insyn och kontroll. Mot registerhanteringen inom Säkerhetspolisen har anmärkningar riktats inte bara av kommissionen utan även av Registernämnden, varvid gjorts gällande att lagstiftningen och tillämpningen av denna i en rad hänseenden inte tillräckligt beaktar rättssäkerhets- och integritetsskyddsaspekter. Registernämndens år 1998 uttalade rekommendation att regeringen borde grundligt överväga hur polisdatalagen skulle kompletteras med föreskrifter i fråga om registrering av uppgifter i Säkerhetspolisens register har ännu inte lett till resultat, i följd varav Registernämndens farhågor att regeringsformens förbud mot åsiktsregistrering överträds alltjämt är relevanta.

Enligt kommitténs uppfattning är det angeläget att de av Säkerhetstjänstkommissionen och Registernämnden påtalade riskerna för olovlig åsiktsregistrering åtgärdas och att pågående arbete med att förstärka den parlamentariska kontrollen slutförs. Innan så har skett skulle det från integritetsskyddssynpunkt framstå som betänkligt att ge Säkerhetspolisen tillgång till nya former av tvångsmedelsanvändning som skulle innebära att ännu mer integritetskänslig information ansamlades hos Säkerhetspolisen. Om Säkerhetspolisen ges möjlighet att använda tvångsmedel också för att förhindra brottslig verksamhet, är en naturlig konsekvens att behovet av 1952 års tvångsmedelslag ses över.

Kapitel 13 Försvarsunderrättelseverksamhet och militär säkerhetstjänst

I kapitlet pekar kommittén på flera förhållanden inom försvarsverksamheten som är otillfredsställande från integritetsskyddssynpunkt. Bland annat påvisas att Försvarets radioanstalts signalspaning till stor del kan utföras utan några som helst författningsenliga begränsningar, både med avseende på vilka uppdragsgivarna kan vara och vilka sökbegrepp och andra parametrar som skall styra verksamheten. Särskilt betänklig är från denna synpunkt den signalspaning som bedrivs vid sidan av försvarsunderrättelseverksamheten. När sådan signalspaning utförs till exempel i brottsbekämpande syfte på uppdrag av Säkerhetspolisen omfattas den inte heller av reglerna för Försvarets underrättelsenämnds tillsyn. En generell brist inom försvarsverksamheten anser kommittén vara att denna verksamhet inte är underkastad någon sekretess-

bestämmelse som syftar till att skydda uppgifter om enskildas personliga och ekonomiska förhållanden inom verksamheten.

Kapitel 14 Gränskontroll

Kommittén konstaterar att sekretessen för fotografier i passregistret relativt nyligen har förstärkts. Härigenom har också integritetsskyddet för passens innehavare förbättrats. Generellt sett måste dock regleringen av behandling av personuppgifter i passregistret anses vara bristfällig. Exempelvis saknas regler om vilka uppgifter registret får innehålla och vad som i övrigt gäller för behandlingen. Reglerna saknar dessutom lagform.

Den utvidgade skyldighet som införts för lufttransportörer att lämna uppgifter om passageraruppgifter har inte heller fått en från integritetsskyddssynpunkt tillfredsställande utformning, eftersom det inte framgår av reglerna vilka skäl som skall ligga till grund för en begäran om uppgifter. Kommittén noterar att det syfte för vilket de aktuella passageraruppgifterna får behandlas, är mycket vagt preciserat i lagen. Detta är olyckligt från integritetsskyddssynpunkt med tanke på att syftet är avgörande för huruvida direktåtkomst får ske och om normal gallringstid får överskridas.

Kommittén bedömer vidare att de lagar som reglerar behandlingen av personuppgifter i Tullverkets fiskala verksamhet, liksom i den brottsbekämpande verksamheten, har utformats utan tillräckligt avseende till vad som gäller enligt det grundläggande regelsystem som finns i sekretesslagen. Förhållandet kan leda till oklarheter om vad som gäller i fråga om utlämnande av uppgifter. Anmärkningsvärt är också att de brottsbekämpande enheterna inom Tullverket har medgivits åtkomst till databasen i den fiskala verksamheten, den så kallade tulldatabasen, utan att integritetsskyddsfrågorna, såvitt framgår, blivit tillräckligt och klart belysta.

Kapitel 15 Hantering av post och elektroniska kommunikationstjänster

I detta kapitel finner kommittén bland annat att integritetsskyddet vid hantering av abonnentuppgifter inom ramen för elektronisk kommunikation i vissa avseenden inte når upp till den nivå som lagstiftaren har avsett. Förhållandet har samband med de grund-

lagsändringar som infördes år 2003, varigenom envar gavs möjlighet att på ett enkelt sätt skaffa sig grundlagsskydd för uppgifter som lämnas via Internet. Följden har blivit att de regler som tillgodoser integritetsskyddet i lagen om elektronisk kommunikation i betydande utsträckning har satts ur spel.

Kommittén konstaterar också att det våren 2006 antagna EG-direktivet om lagring av teletrafikuppgifter kommer att försvaga skyddet för den personliga integriteten. Anledningen är att Sverige måste införa en lagstadgad skyldighet att samla in teletrafikuppgifter i större omfattning och lagra dessa under längre tid än vad som är tillåtet i dag då teleoperatörerna i eget intresse sparar vissa uppgifter av framför allt debiteringstekniska skäl. En ökad informationsvolym innebär också allmänt sett en ökad risk för läckage av känsliga uppgifter till obehöriga och för så kallad ändamålsglidning, dvs. att informationen småningom kommer att användas för något annat samhällsnyttigt ändamål än den varit avsedd för.

Kapitel 16 Allmän kameraövervakning

Kommittén konstaterar att lagen om allmän kameraövervakning föreskriver samma integritetsskydd vid övervakning av exempelvis en arbetsplats eller i en skollokal där hundratals människor vistas dagligen, som vid helt privat övervakning i ett enskilt hem. En sådan brist på precision i lagstiftningen är inte ändamålsenlig utan leder i det ena fallet till ett för svagt och det i andra fallet till ett oproportionerligt starkt integritetsskydd.

Från integritetsskyddssynpunkt är det enligt kommitténs mening inte heller acceptabelt att möjligheten att använda dold övervakning med stöd av reglerna i lagen om allmän kameraövervakning fortfarande kvarstår, trots att lagstiftaren sedan länge varit på det klara med att möjligheten till dold övervakning borde regleras uteslutande genom lagen om hemlig kameraövervakning. Lagstiftarens passivitet i detta avseende har i praktiken fått till följd att det är möjligt att anordna dold kameraövervakning med kringgående av den strängare integritetsskyddsprövning som gäller enligt lagen om hemlig kameraövervakning.

Kapitel 17 Hälso- och sjukvård

Kommittén inleder med att slå fast att det kommer att få stor betydelse för integritetsskyddet på detta område i vad mån själva utgångspunkten för all hälso- och sjukvård – patientens rätt till självbestämmande och integritet – tas i beaktande i det reformarbete som har inletts genom Patientdatautredningens arbete.

Inom hälso- och sjukvården har en väsentlig försvagning av integritetsskyddet skett genom nyligen införda ändringar i sekretesslagen som syftar till ett ökat utlämnande av uppgifter till brottsutredande myndigheter. I detta sammanhang har också vittnesplikten i domstol för viss hälso- och sjukvårdspersonal utökats väsentligt. Kommittén konstaterar att dessa försvagningar av integritetsskyddet har gjorts utan att behoven av ett utökat uppgiftsutlämnande har redovisats på ett tillfredsställande sätt och utan att konsekvenserna för integritetsskyddet har analyserats.

Inom den psykiatriska tvångsvården har reformer genomförts i syfte att stärka patienternas rättssäkerhet och integritet. Socialstyrelsens tillsyn över huruvida kraven på rättssäkerhet uppfylls inom vården synes emellertid inte fungera väl. Detta förhållande finner kommittén betänkligt från integritetssynpunkt, särskilt med tanke på att flertalet av de tvångsåtgärder som vidtas inom vården inte kan överklagas.

Vad särskilt gäller den kategori av patienter som saknar förmåga att själva ta ställning till frågor om vård och behandling bedömer kommittén att respekten för individens självbestämmande och integritet inte kan anses vara tillräckligt beaktad så länge som det i lagstiftningen saknas regler om legala ställföreträdare.

Kapitel 18 Forskning och statistik

I kapitlet konstateras att sekretessreglerna på forskningsområdet är svåröverskådliga och fragmentariska. Förhållandet innebär bland annat svårigheter för forskningshuvudmännen att ge forskningspersonerna korrekt information om vad som kommer att gälla i fråga om skydd för personernas uppgifter. Den nyligen införda etikprövningslagen har inte heller fått en alltigenom tillfredsställande utformning. Det är oklart vilka villkor rörande skydd för den enskilde som enligt lagen bör ställas upp vid etikprövningen, och lagen har fått ett så snävt tillämpningsområde att forskning

som tidigare etikprövades nu inte blir föremål för någon prövning alls. Från integritetsskyddssynpunkt är det också otillfredsställande att lagen medger integritetskänslig forskning på personer som inte har förmåga att själva lämna samtycke och som heller inte har legala ställföreträdare utsedda för sig.

Införandet av lagen om genetisk integritet innebar en förstärkning av integritetsskyddet inom forskningen. Emellertid får det anses som en brist att det i lagen inte klart anges vem som har tillsynsansvaret för hela lagens efterlevnad. Lagen saknar också en heltäckande bestämmelse om den enskildes rätt vid kränkningar som består i att lagens regler inte efterlevs.

Kapitel 19 Socialtjänst

I detta kapitel konstaterar kommittén att behandling av personuppgifter inom socialtjänsten är utförligt reglerad. Uppgifter om enskildas personliga förhållanden omfattas av sträng sekretess, och integritetsskyddet kompletteras av regler om hur handläggning och dokumentation skall ske. Trots dessa förtjänster är skyddet för den personliga integriteten bristfälligt i vissa avseenden.

Sålunda är sekretessgränserna inom socialtjänstområdet otydliga, vilket skapar osäkerhet och risk för ett otillåtet stort utbyte av känslig information. Förhållandet mellan bestämmelserna om barns rätt att komma till tals och om föräldrarnas rätt att besluta för barnets räkning är otydligt uttryckt i lagstiftningen och i vissa avseenden motsägelsefullt, vilket kan leda till omotiverade integritetsförluster för barnen. Vid nyligen företagna förändringar i sekretesskyddet på socialtjänstområdet förefaller integritetsskyddet inte ha värderats och avvägts mot effektivitet och andra motstående intressen i den utsträckning som hade bort ske på detta mycket integritetskänsliga område.

Kapitel 20 Skola och skolhälsovård

För kommittén står det klart att den nya lagstiftningen till skydd för kränkningar av elever har inneburit en förbättring av skyddet för den personliga integriteten. En riskfaktor från integritetsskyddssynpunkt är dock att dokumentationen om enskilda elever liksom tillgängligheten till denna dokumentation ökar i den ordina-

rie undervisningen. Mot den bakgrunden kan det ifrågasättas om skolsekretessens avgränsning till uppgifter i den elevvårdande verksamheten är ändamålsenlig. En annan brist, som kan gå ut över elevernas rätt till integritet, är att skolpersonalens befogenheter att ingripa för att säkerställa ordning och säkerhet i skolan inte är reglerade på ett tillräckligt tydligt sätt.

Barnkonventionens krav på att barn skall ha rätt till likvärdigt skydd för sitt privat- och familjeliv, oberoende av skolform, beaktas inte i full omfattning i lagstiftningen. Även om problemet kan framstå som svårlöst är det från integritetssynpunkt inte tillfredsställande att elever i kommunala skolor åtnjuter ett sämre skydd än friskolornas elever.

Kapitel 21 Socialförsäkring

I detta kapitel konstaterar kommittén att det regelsystem som styr socialförsäkringen är omfattande, svårtillgängligt och i vissa avseenden otydligt och inkonsekvent. Sammantaget innebär detta en ökad risk för att den enskildes personliga integritet kränks i handläggningen och att oriktiga beslut fattas. Felaktiga utbetalningar kan ge anledning till utredningar som orsakar svåra och ibland onödiga ingrepp i den personliga integriteten. Den ofantliga mängd känsliga personuppgifter som hanteras i socialförsäkringssystemet motiverar att behandlingen av personuppgifter regleras genom särlagstiftning. Även denna lagstiftning är emellertid svårtillgänglig vilket kan få negativa integritetsskyddskonsekvenser för den enskilde och försämra dennes möjligheter att bevaka sina intressen. Vidare noterar kommittén att Försäkringskassans informationsutbyte med andra myndigheter är omfattande och fortlöpande utökas. En ambitiös utvärdering av konsekvenserna för enskildas personliga integritet skulle behöva göras för att få underlag för en korrekt bedömning av i vad mån värdet av det ökade informationsutbytet står i proportion till dessa negativa konsekvenser.

Kapitel 22 Arbetslivet

Det saknas ett sammanhållet regelverk som tydligt anger var gränserna går för arbetssökandes och arbetstagares integritetsskydd. I vissa avseenden är det även oklart vad som rättsligt sett gäller,

exempelvis i fråga om drogtester på arbetsplatsen. Dessa brister har länge varit kända. Från integritetsskyddssynpunkt är det angeläget att det utredningsarbete som för närvarande pågår på området leder till resultat.

Kapitel 23 Massmedier och Internet

Utan att anlägga någon egen värdering av frågan konstaterar kommittén att den vidsträckta tryck- och yttrandefrihet som garanteras genom våra grundlagar har ett pris i form av ett allmänt sett ganska svagt skydd för den enskildes privatliv. Den som får sin integritet kränkt i de grundlagsskyddade medierna har generellt sett små möjligheter att få upprättelse, såväl i ekonomiskt som i ideellt hänseende.

I ett avseende är integritetsskyddet emellertid svagare än vad det skulle behöva vara. År 2003 infördes nämligen grundlagsändringar som syftade till att genom en utvidgning av det så kallade databasskyddet ytterligare stärka yttrandefriheten men som fick till konsekvens att den som får sin integritet kränkt genom att uppgifter, bilder eller filmer läggs ut på Internet av en användare som skaffat sig ett frivilligt grundlagsskydd, i praktiken nästan aldrig kan göra gällande någon rätt till upprättelse. Det måste betecknas som en brist under lagstiftningens utarbetande att dessa och andra med lagändringen sammanhängande försämringar av integritetsskyddet inte alls berördes i det aktuella kommittébetänkandet eller i regeringens proposition i ärendet.

Det är vanskligt att säga vad resultatet skulle ha blivit om lagstiftningens konsekvenser fullt ut hade stått klara för regeringen och riksdagen i det aktuella lagstiftningsärendet. I vilket fall som helst konstaterar kommittén för sin del att de berörda grundlagsändringarna har bidragit till en väsentlig försämring av integritetsskyddet på det mediala området.

Kapitel 24 Sammanfattande analys

I detta kapitel sammanfattar kommittén, på sätt framgår av den föregående redogörelsen, sin analys av det sakliga innehållet i sådan lagstiftning som berör den personliga integriteten.

Kommittén uppehåller sig i kapitlet även relativt ingående vid frågor om hur lagstiftning på området har arbetats fram, vilket beredningS- och beslutsunderlag som har funnits tillgängligt för regering och riksdag samt vilka överväganden som i skilda fall lett fram till att balanspunkten har satts på det ena eller andra sättet mellan integritetsskyddsintresset och andra intressen. Särskilt analyserar kommittén hur proportionalitetsprincipen, som ingår i både regeringsformen och Europakonventionen, har tillämpats. Exempel ges på fall där behovet av ny eller ändrad lagstiftning inte på ett tillfredsställande sätt har vägts mot uppkommande negativa effekter för den personliga integriteten. Förklaringen till att en korrekt proportionalitetsbedömning saknas har inte sällan varit att det helt enkelt inte har tagits fram något underlag som gjort det möjligt att närmare bedöma de effekter som påverkar integritetsskyddet. Vid sidan härav framför kommittén åtskilliga andra anmärkningar av system- och metodkaraktär och påvisar hur brister i dessa hänseenden har lett till ett sämre integritetsskydd än vad som hade behövt vara fallet.

På den i direktiven ställda frågan om skyddet för den personliga integriteten kan anses tillfredsställande reglerat, ger kommittén i detta sammanfattande kapitel ett klart nekande svar. Kommittén uttalar en förhoppning om att dess kartläggning och analyser kommer att öka medvetandet om integritetsskyddsaspekternas betydelse i lagstiftningsarbetet. Den genomgång som kommittén redovisar och den kritik som den i vissa avseenden framför bör enligt kommitténs mening kunna tjäna till ledning för det framtida lagstiftningsarbetet och bidra till att undvika icke sakligt motiverade integritetsförluster.

Appendix – Integritetsskyddet i samhällsdebatten

Detta avsnitt innehåller en översikt över efterkrigstidens svenska integritetsskyddsdebatt och ger på så sätt en allmän bakgrund till utredningsuppdraget.

Kapitel 25 – 39 Regelverket

I denna del av betänkandet redogör kommittén mer ingående för sådan lagstiftning som berör skyddet för den personliga integriteten på flertalet av kartläggningsområdena. Det är inte nödvändigt att ta del av denna redogörelse för att förstå kommitténs analys i kapitlen 5–24.

Inledning

1 Utredningsuppdraget

1.1 Kommitténs direktiv

I Integritetsskyddskommitténs direktiv anges att kommittén skall

- kartlägga och analysera sådan lagstiftning som rör den personliga integriteten,
- överväga om regeringsformens bestämmelse om skyddet för den personliga integriteten i 2 kap. 3 § andra stycket bör ändras, och i så fall föreslå en ny grundlagsreglering, samt
- överväga om det, vid sidan av befintlig lagstiftning, behövs generellt tillämpliga bestämmelser till skydd för den personliga integriteten, och i så fall lämna förslag till en sådan reglering.

Integritetsskyddet i förhållande till de grundlagsskyddade massmedierna omfattas enligt direktiven inte av uppdraget. Kommitténuppdraget anges närmare i direktiven enligt följande:

> I kartläggningen ingår att göra en översiktlig undersökning av hur integritetsaspekten har hanterats och reglerats i den lagstiftning som gäller i dag, både på det offentligrättsliga och på det privaträttsliga området. I denna uppgift ingår att se om syftet med reglerna är att förhindra kränkningar eller att kompensera den som kränkts, dvs. om reglerna har en preventiv eller reparativ funktion.
>
> Med utgångspunkt i denna kartläggning skall kommittén analysera om skyddet för den personliga integriteten kan anses tillfredsställande reglerat. När det gäller intresset av effektivitet i brottsbekämpningen skall kommittén därvid särskilt analysera förhållandet mellan den totala verkan av befintliga tvångsmedel och övervakningsmetoder och skyddet för den personliga integriteten.
>
> Kommittén skall överväga om regeringsformens bestämmelse om skyddet för den personliga integriteten i 2 kap. 3 § andra stycket bör ändras, och i så fall föreslå en ny grundlagsreglering. Vad som särskilt skall beaktas är om regeln bör ändras så att den får samma slags rättsliga betydelse som de andra fri- och rättigheterna och om den bör utformas så att den inte hänvisar till något visst tekniskt förfarande.

> Därutöver skall kommittén överväga om den befintliga lagstiftningen till skydd för den personliga integriteten behöver kompletteras med generellt tillämpliga bestämmelser, och i så fall lämna förslag till en sådan reglering. Det kan röra sig om straffbestämmelser eller skadeståndssanktionerade regler. Även andra lösningar bör kunna övervägas. Det är däremot inte kommitténs uppgift att lämna förslag på varje särskilt område inom den befintliga lagstiftningen. Om denna visar sig innehålla luckor, bör kommittén emellertid peka på detta vid kartläggningen.

Kommittén skulle enligt direktiven slutredovisa sitt arbete senast den 30 mars 2007. Genom tilläggsdirektiv har utredningstiden förlängts till den 20 december 2007. Båda direktiven återges i sin helhet i *bilagorna 1 och 2*.

1.2 Utredningsarbetet

I förevarande delbetänkande redovisar kommittén uppdraget i den del som avser kartläggning och analys av sådan lagstiftning som rör den personliga integriteten. Kommitténs överväganden rörande behovet av ny lagstiftning kommer att redovisas senare i ett slutbetänkande.

Utredningsarbetet har bedrivits på sedvanligt sätt med regelbundna sammanträden med kommittén i dess helhet. Kommitténs ordförande, sekreterare och experter har haft ett betydande antal arbetsmöten. Det samråd som kommittén förutsatts ha med Tryck- och yttrandefrihetsberedningen (Ju 2003:04) har inletts. Kommitténs sekretariat har inhämtat uppgifter – förutom från tryckta källor – från myndigheter och organisationer samt träffat företrädare för bland annat Rikskriminalens spaningsrotel och Vetenskapsrådets etikkommitté. Trafikutbytesutredningen (Fi 2005:08) har i enlighet med sina direktiv samrått med kommittén. Det har även Brottsförebyggande rådet gjort med anledning av ett regeringsuppdrag rörande så kallad stalking.

Statistiska Centralbyrån har bistått kommittén vid genomförandet av en statistisk undersökning rörande befolkningens inställning till frågor om integritetsskydd, *bilaga 5*. En förstudie till undersökningen utarbetades av Institutet för Rättsinformatik vid Stockholms universitet, *bilaga 4*. Kommitténs redovisning av den tekniska utvecklingen baseras på ett underlag som Datainspektionen har tagit fram på kommitténs begäran.

Den redogörelse som i förevarande betänkande lämnas för befintlig och föreslagen lagstiftning omfattar, med något undantag, tiden fram till den 1 januari 2007.

Kommittén har enligt direktiven haft i uppgift att ”analysera om skyddet för den personliga integriteten kan anses tillfredsställande reglerat”. För att kunna bedöma denna fråga i hela dess vidd har kommittén behövt kartlägga och analysera i princip all lagstiftning som berör den personliga integriteten, dvs. även sådan lagstiftning som innefattar ett grundlagsskydd för massmedierna. En annan sak är att kommittén i sina förestående överväganden rörande behovet av ny lagstiftning till skydd för den personliga integriteten inte har i uppgift att gå in på det grundlagsreglerade området.

1.3 Betänkandets disposition

Delbetänkandet är uppdelat på två volymer. Den första volymen inleds med en redovisning av de utgångspunkter och grundläggande avgränsningar för arbetet som kommittén bedömt vara nödvändiga. Härefter kartläggs och analyseras rättsområde efter rättsområde med avseende på integritetsskyddet. I avsnitt 24 *Sammanfattande analys* redovisar kommittén de allmänna iakttagelser som den har gjort under arbetets gång och sammanställer de iakttagelser och analyser som förekommer i anslutning till varje enskilt rättsområde. Avsnittet avslutas med de övergripande bedömningar som kommittén funnit motiverade.

Till den första volymen fogas ett appendix, som innehåller en exposé över efterkrigstidens svenska integritetsskyddsdebatt.

Den andra volymen innehåller en mer utförlig beskrivning av regelverket på integritetsskyddsområdet samt utredningens direktiv och de övriga bilagor som hör till delbetänkandet.

2 Utgångspunkter och avgränsningar

2.1 Grundläggande regler

I Sverige liksom i många andra rättstater bygger regleringen av enskildas fri- och rättigheter på dels en nationell grundlagsreglering, dels folkrätten och ingångna internationella avtal. I sistnämnda hänseende intar för Sveriges del EG-rätten principiellt sett en särställning, eftersom denna inom sitt tillämpningsområde i händelse av normkonflikt har företräde framför nationell rätt. En särställning intar även Europakonventionen genom att den inte bara har gjorts till en integrerad del av den svenska rättsordningen utan också föranlett ett grundlagstadgat förbud mot lagstiftning i strid med Sveriges åtaganden enligt konventionen.

Nedan redogörs för internationella överenskommelser som Sverige har anslutit sig till och som har betydelse för skyddet av den personliga integriteten. Vidare redovisas de svenska grundlagsbestämmelser som har betydelse för detta skydd.

2.1.1 Internationella bestämmelser

Förenta nationerna

Förenta nationernas (FN) generalförsamling antog år 1948 en universell deklaration om de mänskliga rättigheterna, *Förenta Nationernas allmänna förklaring om de mänskliga rättigheterna*. Deklarationen är inte formellt bindande för medlemsstaterna, men har betydelse som ett uttryck för vad den internationella opinionen kräver. I artikel 12 sägs att ingen ”må utsättas för godtyckliga ingripanden i fråga om privatliv, familj, hem eller korrespondens, ej heller angrepp på heder och anseende” samt att envar ”har rätt till lagens skydd mot sådana ingripanden eller angrepp”.

Vidare sägs i artikel 29 att endast sådana inskränkningar i de i deklarationen angivna fri- och rättigheterna är tillåtna som fastställts i lag ”i uteslutande syfte att trygga tillbörlig hänsyn till och respekt för andras fri- och rättigheter samt för att tillgodose det demokratiska samhällets rättmätiga krav på moral, allmän ordning och allmän välfärd”.

Inom FN har också utarbetats en internationell konvention om medborgerliga och politiska rättigheter, som antogs av generalförsamlingen år 1966. Sverige anslöt sig till konventionen år 1971, varefter konventionen trädde i kraft år 1976. I konventionen behandlas vad som hör till skyddet för den personliga integriteten främst i artikel 17. Enligt denna artikels punkt 1 må ingen ”utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens, ej heller för olagliga angrepp på sin heder och sitt anseende”. Vidare sägs i punkt 2 att envar ”har rätt till lagens skydd mot sådana ingripanden eller angrepp”.

De stater som har tillträtt konventionen åläggs således vissa skyldigheter. Ett särskilt inrättat organ benämnt kommittén för de mänskliga rättigheterna (Human Rights Committee) övervakar att de till konventionen anslutna staterna efterlever sina skyldigheter.

Europarådet

Sverige har inom det europeiska samarbetets ram anslutit sig till *Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna* (Europakonventionen). Av betydelse för skyddet för den personliga integriteten är framför allt artikel 8 som lyder:

> 1. Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens.
>
> 2. Offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och 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.

Primärt innebär artikel 8 att staten skall avhålla sig från ingrepp i den skyddade rättigheten. Artikeln innebär även en skyldighet för staten att vidta positiva åtgärder för att skydda den enskildes

privatsfär. Sådana positiva åtgärder kan utgöras av lagstiftning men också ha till ändamål att på annat sätt tillförsäkra medborgarna skydd mot övergrepp i särskilda situationer (Hans Danelius, *Mänskliga rättigheter i europeisk praxis*, 2 uppl., s. 261 f.). I sin praxis har Europadomstolen också framhållit att kravet på att ingreppet skall vara nödvändigt inte är synonymt med ”oundgängligt”. Vad som krävs är däremot att det finns ett ”angeläget samhälleligt behov”. Inskränkningen i den grundläggande rättigheten måste vidare stå i rimlig proportion till det syfte som skall tillgodoses genom inskränkningen. Varje konventionsstat har själv en viss frihet att avgöra om en inskränkning är nödvändig. Europadomstolen förbehåller sig dock rätten att övervaka om denna frihet utnyttjas på ett rimligt sätt.

I detta sammanhang kan också nämnas artikel 3, enligt vilken ingen får utsättas för tortyr eller omänsklig eller förnedrande behandling eller bestraffning.

Europakonventionen är fr.o.m. 1995 inkorporerad i svensk rätt som vanlig lag (prop. 1993/94:117, bet. 1993/94:KU24). Den har alltså inte getts ställning av grundlag. I 2 kap. 23 § regeringsformen (RF) har emellertid införts en bestämmelse om att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Europeiska unionen

Sverige är sedan den 1 januari 1995 medlem i Europeiska unionen (EU). Enligt artikel 6 i EU-fördraget bygger unionen på principerna om frihet, demokrati och respekt för de mänskliga rättigheterna och grundläggande friheterna samt på rättsstatsprincipen, vilka principer anges vara gemensamma för medlemsstaterna. Av särskild betydelse för medlemsstaterna och medborgarna är att unionen skall som allmänna principer för gemenskapsrätten respektera de grundläggande rättigheterna, såsom de garanteras i Europakonventionen och såsom de följer av medlemsstaternas gemensamma konstitutionella traditioner. Sistnämnda stadgande är primärt riktat till gemenskapslagstiftaren, men genom EG-domstolens praxis har konventionen och Europadomstolens tillämpning av densamma kommit att få ett genomslag i de nationella rättsordningarna som går utöver de rent gemenskapsbaserade reglerna. Rättsligt sett kan detta sägas

innebära att väsentliga delar av Europakonventionens fri- och rättighetssystem via förmedling av EG-rätten har blivit tillämpligt i Sverige såsom EG-rätt och därmed bl.a. kommit i åtnjutande av den företrädesrätt som gemenskapsbestämmelserna har gentemot rent nationell rätt.

Vid Europeiska rådets möte i Nice 2000 antog medlemsstaterna *Europeiska unionens stadga om de grundläggande rättigheterna* (EU-stadgan). Stadgan anger bland annat att var och en har rätt till fysisk och mental integritet (artikel 3), respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer (artikel 7) samt skydd av de personuppgifter som rör honom eller henne (artikel 8). I fördraget 2003 om upprättande av en konstitution för Europa anges att stadgan riktar sig till unionens institutioner samt till medlemsstaterna ”endast när dessa tillämpar unionsrätten”, artikel II-51. I fördraget anges också att unionen skall söka anslutning till Europakonventionen, artikel 7. Fördraget hade vid ingången av år 2007 ratificerats av 18 av EU:s medlemsstater. Efter att medborgarna i Frankrike och Nederländerna röstade nej till fördraget är det ovisst om fördraget kommer att antas.

2.1.2 Svenska grundlagsbestämmelser

Det allmänna skall värna den enskildes privatliv och familjeliv

Före tillkomsten av den nu gällande regeringsformen, som slutligen antogs 1974, var det endast tryckfriheten som av de medborgerliga fri- och rättigheterna hade något egentligt grundlagsskydd. I 1809 års regeringsform gavs visserligen i 16 § uttryck för vissa åldriga principer om den enskildes skydd mot ingrepp från statsmaktens sida. I paragrafen angavs bl.a. att Konungen bör ”ingens samvete tvinga eller tvinga låta”. Bestämmelsen ansågs dock knappast innefatta någon garanti i rättslig mening för medborgarnas fri- och rättigheter (prop. 1973:90 s. 192).

Gällande grundlag innehåller inte heller någon rättsligt bindande regel som innebär ett allmänt integritetsskydd. Genom 1976 års regeringsform infördes däremot ett målsättningsstadgande i 1 kap. 2 § där vissa för medborgarna grundläggande värden slogs fast. I denna paragraf angavs att den offentliga makten bör utövas så att den enskildes privat- och familjeliv skyddas. Stadgandet återfinns

numera i 1 kap. 2 § fjärde stycket RF, där det sägs att det allmänna skall ”värna den enskildes privat- och familjeliv”.

Fri- och rättighetsutredningen, vars förslag låg till grund för bestämmelsen i 1 kap. 2 § RF, framhöll i sitt betänkande *Medborgerliga fri- och rättigheter* (SOU 1975:75) att det i betydande utsträckning redan fanns ett skydd för vad som kan kallas enskilds privatliv eller personliga integritet genom de regler som införts genom 1974 års regeringsform och som skyddade mot sådana åtgärder från det allmännas sida som husrannsakan, intrång i brev, post- och teleförbindelser samt hemlig avlyssning (s. 168 f.). Utredningen påpekade också att detta skydd kunde komma att förstärkas genom utredningens förslag om ett förbud mot åsiktsregistrering. Detta förbud var visserligen främst avsett att ingå som ett moment i skyddet för åsiktsfriheten, men verkade också som ett skydd för den enskildes personliga integritet.

Utredningen underströk att begreppet personlig integritet visserligen förekom i svensk lagstiftning. Det hade dock inte kunnat ges någon klar avgränsning. Enligt utredningen framstod därför ett allmänt integritetsskydd i grundlagen som uteslutet, om det skulle utformas som en rättsregel. Emellertid ansåg utredningen att principen att den enskilde bör ha tillgång till en fredad sektor är så grundläggande i en demokrati att den borde komma till uttryck i grundlagen, detta trots att den enskildes rätt att bli lämnad i fred aldrig kan vara absolut i ett samhälle och trots att den enskildes privata sektor måste begränsas av gemenskapens krav. Principen borde därför tas upp i ett målsättningsstadgande i regeringsformen som slog fast vissa för medborgarna grundläggande värden.

Förbud mot åsiktsregistrering samt skydd för kroppsliga fri- och rättigheter

Som framgått innehåller regeringsformen, vid sidan av målsättningsstadgandet i 1 kap. 2 § om att det allmänna skall värna den enskildes privatliv och familjeliv, rättsligt bindande regler som i vissa delar utgör ett skydd för den personliga integriteten. Ett sådant skydd är stadgandet i 2 kap. 3 § första stycket, där det föreskrivs att anteckning om medborgare i allmänt register inte får grundas enbart på hans politiska åskådning. Förbudet mot

åsiktsregistrering är absolut i den meningen att det inte kan begränsas på annat sätt än genom grundlagsändring.

I 2 kap. RF finns också rättsligt bindande regler som skyddar de ”kroppsliga” fri- och rättigheterna, dvs. skyddet för den enskildes frihet och säkerhet till person. Dit hör rörelsefriheten och skyddet mot kroppsstraff, tortyr och olika slag av kroppsliga ingrepp. Till denna kategori räknas också skydd mot husrannsakan och intrång i post, brev och teleförbindelse samt mot hemlig avlyssning (prop. 1975/76:209 s. 119).

Skyddet för ”kroppsliga” fri- och rättigheter fungerar i betydande utsträckning som förstärkning av skyddet för de s.k. opinionsfriheterna. I förarbetena framhålls att det t.ex. är tydligt att föreskrifter som skyddar den enskildes rörelsefrihet indirekt också skyddar hans möjligheter att utöva sin yttrandefrihet, demonstrationsfrihet etc. (a. prop. s. 119). Fördragande statsrådet påpekade att det emellertid är uppenbart att bestämmelserna om de kroppsliga fri- och rättigheterna även har verkan utanför det område som avser skyddet för demokratin. De ger också uttryck för den respekt för den enskilda individens integritet som är utmärkande för ett rättssamhälle.

Några av grundlagsreglerna till skydd för den kroppsliga integriteten är absoluta. Hit hör förbuden mot dödsstraff i 2 kap. 4 § RF och kroppsstraff i 2 kap. 5 § RF. Varje medborgare är enligt sistnämnda lagrum också skyddad mot tortyr och mot medicinsk påverkan i syfte att framtvinga eller hindra yttranden.

Övriga grundlagsregler till skydd för den kroppsliga integriteten är relativa. De kan alltså begränsas genom vanlig lag enligt bestämmelserna i 2 kap. 12 § RF. Till denna kategori hör regeln i 2 kap. 6 § om att varje medborgare även i annat fall än som avses i 4 och 5 §§ är skyddad mot påtvingat kroppsligt ingrepp. Hit hör också skyddet enligt samma paragraf mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande.

Fri- och rättigheterna enligt 2 kap. 6 § får alltså enligt 2 kap. 12 § begränsas, men i så fall endast genom lag och bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En sådan rättighetsbegränsande lagstiftning får aldrig gå utöver vad som är nödvändigt med hänsyn till ändamålet och inte heller sträcka sig så långt att lagstiftningen utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras

enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

I förarbetena betonades att regleringen i 2 kap. 12 § RF är ägnad att understryka kravet på att lagstiftaren, när en fri- och rättighetsinskränkande lag beslutas, noga redovisar sina syften (prop. 1975/76:209 s. 153).

Regleringen i 2 kap. 12 § RF har bl.a. legat till grund för den ändamåls-, behovs- och proportionalitetsprincip som anses gälla för det allmännas användning av tvångsmedel enligt bestämmelserna i rättegångsbalken. Ett annat exempel är den proportionalitetsprincip som gäller vid användning av tvångsåtgärder inom den psykiatriska tvångsvården.

Skyddet för de fri- och rättigheter som omfattas av 2 kap. 6 § RF har genom ändringar i regeringsformen år 1979 förstärkts på så sätt att det i 2 kap. 12 § tredje stycket införts regler om ett särskilt förfarande vid antagandet av rättighetsbegränsande lagstiftning. Med undantag för vissa särskilt angivna fall gäller att förslag till sådan lagstiftning, om det begärs av minst tio riksdagsledamöter, skall vila i minst tolv månader hos riksdagen innan det får antas. Om förslaget vid en första omröstning får stöd av minst fem sjättedelar av de röstande blir det dock omedelbart antaget.

Skydd mot integritetskränkande dataregistrering

År 1988 infördes i 2 kap. 3 § andra stycket RF en bestämmelse om skydd mot integritetskränkande databehandling. Där föreskrivs att varje medborgare skall i den utsträckning som närmare anges i lag skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Rättsligt sett innebär bestämmelsen endast att lagstiftaren är skyldig att på det aktuella området upprätthålla ett skydd för den personliga integriteten. Grundlagsbestämmelsen får härigenom karaktär av normgivningsregel, medan de skyddsregler som skall finnas på området får sökas i vanlig lag, framför allt i personuppgiftslagen (1998:204).

2.2 Begreppet personlig integritet – en avgränsning

Vid diskussioner om hur den enskildes integritet skall skyddas är en ständigt återkommande fråga vad som egentligen avses med detta begrepp. En sådan begreppsanalytisk infallsvinkel har emellertid sina begränsningar. Ett skäl härtill är att det, som närmare kommer att framgå av det följande, är svårt för att inte säga omöjligt att komma fram till en entydig och allmänt accepterad definition av begreppet personlig integritet. Ett annat skäl är att man inte genom att bestämma innebörden av detta begrepp ens teoretiskt kan få svar också på frågan om vad det är som skall skyddas. Den sistnämnda frågan kan nämligen inte besvaras utan att man samtidigt bedömer omfattningen och tyngden av de motstående legitima intressen som kan finnas, såsom intresset av offentlighet och brottsbekämpning.

Utformandet av ett integritetsskydd, i Sverige såväl som på andra håll, synes heller inte i praktiken ha tagit sin utgångspunkt i en viss definition av begreppet integritet, utan arbetet har varit inriktat på att från fall till fall förbjuda sådana företeelser som inte ansetts försvarbara med hänsyn till dels den skada de skulle innebära för den personliga integriteten, dels den skada som ett upprätthållande av integriteten skulle åsamka andra beaktansvärda intressen. I rättsordningen har med andra ord den faktiska omfattningen av den skyddade personliga integriteten kommit att bestämmas inte genom sofistikerade definitioner utan genom summan av ett stort antal skyddsregler av mycket varierande slag.

Det sagda förminskar på intet sätt värdet av att studera de försök till begreppsbestämningar rörande den personliga integriteten som tidigare har gjorts. För kommittén är det nödvändigt att hålla sig till en arbetshypotes som på något sätt gränsbestämmer omfattningen av vad som skall kartläggas och analyseras, varvid inspiration och ledning kan sökas i de olika uppfattningar som förekommer rörande innebörden av begreppet personlig integritet. Det kan redan här sägas att kommittén inte har funnit det meningsfullt att formulera någon egen heltäckande definition av detta begrepp.

Det bör framhållas att personlig integritet inte är det enda begrepp som förekommer i detta sammanhang. Exempelvis använde 1966 års integritetsskyddskommitté begreppet ”privatlivets fred”, och Europakonventionen talar om att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin

korrespondens. EU-stadgan föreskriver ett motsvarande skydd samt dessutom en rätt till fysisk och mental integritet och till skydd av egna personuppgifter. Finlands nya grundlag anger att alla har rätt till integritet och, i ett annat lagrum, att vars och ens privatliv, heder och hemfrid är tryggad. Uppenbarligen används dessa och liknande begrepp med varierande innebörd och med delvis överlappande syftning.

I anslutning till det sistnämnda kan det framhållas att den engelska termen ”privacy”, som ibland åberopas i integritetsdebatten, torde ha en något vidare syftning än vad som hos oss i allmänhet menas med personlig integritet och täcka in även vad som kan kallas personligt oberoende och självständighet.

2.2.1 Allmän karaktäristik av begreppet personlig integritet

I Svenska Akademiens ordlista beskrivs ordet integritet som orubbat tillstånd; okränkbarhet; oberoende.

Av Nationalencyklopedin framgår att ordet integritet kommer av latinets *integritas* och står för orörd, hel, fullständig, oförvitlig, hederlig. Ordet ges fyra olika betydelser, däribland rätten att ”få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp (personlig integritet)”.

På Datainspektionens hemsida ges följande beskrivning av begreppet personlig integritet: Det finns ingen allmänt vedertagen definition, integritet är en inre egenskap, som är olika hos olika individer. ”Rätten att få vara i fred” är en vanlig tolkning. ”Rätten att få sin personliga egenart och inre sfär respekterad och inte utsättas för kränkande behandling” är en annan.

Den statliga utredning som senast hade anledning att resonera kring integritetsbegreppet, Integritetsutredningen, gjorde i betänkandet *Personlig integritet i arbetslivet* (SOU 2002:18) följande överväganden beträffande ”vad som egentligen innefattas i begreppet personlig integritet” (s. 52 f.):

> Utredningen har gjort en genomgång av åtskillig svensk och utländsk litteratur i ämnet för att söka finna svaret på denna fråga. Det har emellertid visat sig att begreppet personlig integritet inte är så lättfångat. Stora ansträngningar har gjorts för att definiera det men något kortfattad generell konkretisering av begreppets språkliga innebörd har utredningen inte kunnat finna. Men som en klar gemensam nämnare framstår i vart fall uppfattningen att begreppet

personlig integritet innebär att alla människor har rätt till en personlig sfär där ett oönskat intrång, såväl fysiskt som psykiskt, kan avvisas.

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

Justitierådet Per Jermsten gjorde följande reflektioner i departementspromemorian *Skyddet för enskilda personers privatliv* (Ds Ju 1994:51 s. 8 f.).

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

2.2.2 Integritetsbegreppet i andra sammanhang

Europakonventionen

I sin kommentar till Europakonventionen och den praxis som utbildats vid dess tillämpning framhåller Danelius (a.a., s. 260 f.) i anslutning till artikel 8 att rätten till respekt för privatlivet är en svårdefinierad rättighet med många aspekter. Många olika företeelser kan, om man så vill, hänföras till privatlivet och först genom rättspraxis kan begreppet få en någotsånär tydlig avgränsning. Författaren påpekar att många av de rättigheter som behandlas i andra artiklar i konventionen och dess tilläggsprotokoll kan sägas beröra privatlivet, t.ex. skydd mot tortyr och omänsklig

eller förnedrande behandling (artikel 3) och frihetsberövande (artikel 5). Artikel 8 fångar endast upp de aspekter av privatlivet som faller utanför specialbestämmelserna.

Vid sidan av rätten till respekt för privatlivet behandlas i artikel 8 också rätten till respekt för familjelivet samt för hem och korrespondens. Dessa rättigheter är enligt Danelius nära förbundna med rätten till respekt för privatlivet och kan ofta inte särskiljas från denna rättighet (a.a., s. 261).

Artikel 8 har genom Europadomstolens praxis kommit att tillämpas på en mängd olika företeelser. Rätten till respekt för privatlivet omfattar bl.a. en persons fysiska integritet, dvs. rätten att vara fri från kroppsliga övergrepp (skydd mot allvarligare övergrepp finns i artikel 3). Denna rätt innefattar också krav på strafflagar mot misshandel och sexuella övergrepp. Dock medges att stater i viss mån förbjuder kroppsliga ingrepp som den enskilde i och för sig *vill* undergå, t.ex. könsbyte, transplantation och abort. Rätten till respekt för privatlivet har tillämpats också beträffande tillgång till personuppgifter förvarade hos myndigheter, såväl i fråga om egna som andras privata förhållanden.

När det gäller rätten till respekt för sitt hem har innefattats inte bara skydd för den enskildes bostad, utan också ett bolags lokaler. Människor skall också skyddas mot att bli fördrivna från sina hem och mot att deras bostäder förstörs. Denna rätt innefattar en skyldighet för konventionsstaterna att ingripa mot mer allvarliga störningar i människors boendemiljö.

Rätten till respekt för familjelivet omfattar föräldrar och deras minderåriga barn. Denna rätt har aktualiserats i samband med olika umgängesrättsfrågor, bl.a. i samband med skilsmässa och fängelsevistelse. Den har också ansetts omfatta utländska medborgares rätt till familjeliv i vissa fall. (En närmare redovisning av det område som skyddas av artikel 8 ges, förutom av Danelius i hans anmärkta arbete, av D.I. Fischer i *Mänskliga rättigheter, En introduktion*, 2 uppl. 2003).

Strömholms ”kränkningsförteckning”

Under 1960-talet uppkom i framför allt USA en vetenskaplig diskussion om rätten till ”privacy”, initierad av jurister och forskare som W.L. Prosser och Alan F. Westin, varvid särskilt märks den senares arbete *Privacy and Freedom* från år 1967.

Ett viktigt försök att definiera begreppet integritet gjordes också i vår del av världen i samband med den nordiska konferens om privatlivets rättsskydd som hölls i Internationella juristkommissionens regi år 1967. Resultatet blev en resolution som vunnit internationell uppmärksamhet. Enligt resolutionen innebär rätten till privatliv i allmänhet en rätt för individen att leva sitt eget liv med ett minimum av inblandning från myndigheter, allmänhet och andra individer. Definitionen konkretiseras sedan genom att man systematiserar och anger de typer av integritetskränkningar som kan förekomma.

Denna diskussion fördes vidare och utvecklades i Sverige av bl.a. professorerna Åke Lögdberg (se *Personlighetsrätt*, 1972) och Stig Strömholm (se *Individens skyddade personlighetssfär*/ur Om våra rättigheter, Antologi utgiven av Rättsfonden, 1980, se även SvJT 1971 s. 695).

Strömholm framhåller att intresset för en ”personlighets- eller integritetssfär” långtifrån är ny, och att filosofen Montaigne redan för fyrahundra år sedan skrev: ”Man måste förbehålla sig en liten kammare bakom butiken, en kammare som är helt och hållet vår egen och helt och hållet fri.; där vi upprättar vårt sanna oberoende och vår främsta tillflyktsort och ensamhet…”

När det gällde den aktuella debatten återger Strömholm fyra av Westin utpekade speciella funktioner som ett rättsligt skydd för individens privata sfär bör tillgodose i ett samhälle av modern typ. En ”right of privacy” behövs således för känslan av personlig självbestämmanderätt, för att uppnå känslomässig avkoppling och därmed befrias från det ålagda sociala rollporträttet, för att kunna genomföra en fri värdering av andras och inte minst eget handlande och slutligen för att kunna kommunicera fritt med andra efter eget val.

Strömholm ger följande förklaringar till varför ”privacy”-problematiken hade kommit att få så starkt ökad uppmärksamhet. Till att börja med har väsentligt större delar av befolkningen i industriländerna kommit att leva nära varandra, i ”täta” samhällen på ett sätt som tidigare gällde endast mindre grupper. Ett annat moment är de nya stora samhällenas anonymitet, som lätt uppfattas som hotande. Sannolikt bör man enligt Strömholm också räkna med förändringar i människors sensibilitet och attityder. De ekonomiska och sociala faktorer som faktiskt har förbättrat förutsättningarna för total avskildhet har gjort oss mindre beredda att dela ens något avsnitt av vårt privatliv med andra. Men det finns

också tendenser till ”avprivatisering” av livsområden, som tidigare förbehölls en trängre krets; t.ex. på badstränder och vid begagnandet av kommunikationsmedel.

Ett annat starkt motiv för tillgång till ett effektivt skyddat privatliv är enligt Strömholm de ökade eller kanske snarare till sin inriktning förändrade krav som individen har att möta utanför den skyddade kretsen. Det demokratiska samhällsskicket, vars former spritts till allt bredare områden, kräver åtminstone idealtypiskt människor som lämnar självständiga bidrag till kollektivet. Skall dessa anspråk kunna realiseras är det nödvändigt att var och en kan dra sig tillbaka till sin ”kammare bakom butiken” både för att helt enkelt koppla av, slippa ifrån den sociala rollen och för att överväga sin egen ståndpunkt i beslutsfrågor där den egna medverkan krävs. Den offentliga masskommunikationens dygnsomfattande och högröstade tryck borde på samma sätt öka behovet av en sfär, där förtrolig kommunikation på egna villkor är möjlig.

Till de allmänna förändringar i levnadsbetingelserna som ger ökad aktualitet och styrka åt den enskildes krav på en skyddad ”personlighetssfär” kommer enligt Strömholm nya former för intrång i vad som tidigare kunde räknas som i praktiken oåtkomligt område. Westin anger särskilt tre former för sådana intrång som kommit att prägla den moderna debatten om personlighetsskyddet. Först och främst har med olika tekniska hjälpmedel möjligheterna för fysisk övervakning drastiskt utvidgats. För det andra har datorteknikens utveckling möjliggjort lagring och sammanställning av praktiskt taget obegränsade informationsmängder av ett slag som tidigare oftast fanns utspritt i talrika mer eller mindre svårtillgängliga manuellt förda arkiv. Som en tredje ny övervakningsform betecknar Westin de olika typer av tester och psykologiska undersökningar som kommer till användning vid rekrytering av elever, personal osv.

Strömholm framhåller att den integritets- eller personlighetssfär som avses i den moderna diskussionen och i moderna rättsordningar inte kan knytas till vare sig speciella dokument, uppteckningar e.d., speciella människor – enligt indelningen i ”offentliga personer” och ”privatpersoner” – lokaler (”privat område osv.) eller verksamheter. Det är inte minst denna relativitet som gör integritetsbegreppet så svåråtkomligt för lagstiftare och juridiska beslutsfattare, vilka av principiella skäl söker efter enhetliga och generella kriterier för sina lösningar. Jurister har därför ofta resignerat inför uppgiften att ge en positiv bestämning

av personlighets- och integritetsbegreppen. I stället har de försökt beskriva dessa begrepp på ett negativt sätt, genom att göra förteckningar över de handlingar som kan anses utgöra integritetskränkningar. Som framgår även av kommitténs direktiv har Strömholm själv gjort en sådan förteckning, vilken har åberopats i åtskilliga sammanhang då begreppet personlig integritet har diskuterats.

Enligt Strömholms ”kränkningsförteckning” kan kränkningarna indelas i tre huvudgrupper: 1) intrång, vare sig i fysisk eller annan mening, i en annan persons privata sfär; 2) insamlande av uppgifter om en persons privata förhållanden; 3) offentliggörande eller annat utnyttjande (t.ex. som bevis inför rätta, som medel för utpressning) av material om en persons privata förhållanden. Mer konkret kräver följande grupper av handlingar beaktande:

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

Med andra ord skulle, menar Strömholm, ”privatsfären” eller ”integritetssfären” kunna beskrivas såsom inbegreppet av de intressen vilka kränks eller åtminstone kan kränkas genom de uppräknade handlingarna. I en mycket grov sammanfattning skulle denna ”sfär” sålunda vara en ”beteckning för den enskildes intresse av att själv och ensam så att säga reglera dels flödet av den information som utgår beträffande hans förhållanden, dels utnyttjandet av sådan information samt av speciella identifikationsdata (namn, bild, röst)”.

1966 års integritetsskyddskommitté

I betänkandet *Skydd mot avlyssning* (SOU 1970:47) menade 1966 års integritetsskyddskommitté att grundtanken med personlig integritet torde kunna uttryckas så, att den enskilde kan göra anspråk på en fredad privat sektor inom vilken han kan avvisa inblandning från utomstående. Integritetsbegreppet kunde i det sammanhanget ses som liktydigt med den enskildes anspråk att information om hans privata angelägenheter inte skall vara tillgänglig för eller få begagnas av utomstående mot hans vilja (s. 58). Kommittén konstaterade själv att denna bestämning emellertid inte innebär mer än en ram inom vilken den enskildes privatliv kan skyddas mot angrepp. I vad mån sådant skydd verkligen borde beredas den enskilde berodde därutöver på en avvägning av den enskildes integritetsanspråk mot det intresse som föranledde angreppet.

Kommittén underströk särskilt att den gjorda bestämningen av integritetsbegreppet inte syftade till att närmare ange vilka företeelser som borde betraktas som den enskildes privata angelägenheter. Det torde enligt kommittén inte heller vara möjligt att åstadkomma en komplett uppräkning av dessa företeelser. Praktiskt sett hängde frågan samman med arten av det angrepp som hotade den enskilde. Frågan fick lösas i samband med att olika angreppsformer behandlades.

Vidare framhöll kommittén att det integritetsbegrepp av generell räckvidd som kommittén hade angett främst var uttryck för en grundläggande rättspolitisk värdering. Samtidigt gav det en allmän föreställning om de slag av intressen som åsyftas.

I sitt slutbetänkande *Privatlivets fred* (SOU 1980:8) återkom kommittén till begreppsfrågan. Kommittén konstaterade (s. 70 f.)

att åtskilliga försök hade gjorts att definiera integritetsbegreppet och hänvisade bl.a. till Strömholms ovan nämnda indelning i olika handlingstyper som medförde intrång i den personliga integriteten. Kommittén hänvisade emellertid även till ett engelskt lagförslag från år 1969 som innehöll följande definition:

> Rätt till privatliv innebär rätt för envar till skydd mot intrång riktat mot hans person, hem, familj, egendom och affärsangelägenheter samt mot hans relationer och kommunikationer med andra; i synnerhet när intrånget företas genom (a) spioneri, snokande, övervakning eller annat ofredande, (b) olovlig avlyssning eller registrering av samtal, (c) olovlig avbildning, (d) olovlig läsning eller kopiering av handlingar, (e) olovlig användning eller olovlig avslöjande av förtroliga uppgifter eller av omständigheter (inräknat namn, identitet och bild) när avsikten antingen är att orsaka honom obehag, förargelse eller förlägenhet eller att få honom att framstå i falsk dager samt (f) olovlig utnyttjande av namn, identitet eller bild för annans vinning.

I anslutning till denna definition framhöll kommittén att dess första betänkande – *Skydd mot avlyssning* (SOU 1970:47) – avsåg sådana kränkningar som sker genom ”olovlig avlyssning” (b). Det andra betänkandet – *Fotografering och integritet* (SOU 1974:85) – behandlade intrång som kommer till stånd genom ”olovlig avbildning” (c) och såvitt avsåg delavsnittet om TV-övervakning närmast intrång genom ”övervakning” (a). I betänkandet *Reklam och integritet* (SOU 1978:48) föreslog kommittén åtgärder mot intrång som närmast överensstämde med kategori (f), dvs. för kommitténs del olovligt utnyttjande av namn eller bild för annans vinning. Kommitténs slutbetänkande, som handlade om de problem som var förenade med det intrång i privatlivet som sker genom användning och spridning av integritetskränkande material, avsåg närmast intrång som kunde hänföras till kategori (e) i det engelska lagförslaget.

Tvångsmedelskommittén

Tvångsmedelskommittén, som hade till uppgift att göra en översyn av tvångsmedelsregleringen vid förundersökningen i brottmål, använde sig i betänkandet *Tvångsmedel, anonymitet, integritet* (SOU 1984:54) av följande indelning av begreppet integritet som utgångspunkt för sitt arbete (s. 42 f.):

- den rumsliga integriteten (hemfrid, jfr 2 kap. 6 § RF),
- den materiella integriteten (egendomsskydd, jfr 2 kap. 18 § RF),
- den kroppsliga integriteten (skydd för liv och hälsa, mot ingrepp i eller mot kroppen, kroppsvisitation, kroppsbesiktning m.m., jfr 2 kap. 6 § RF),
- den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten, jfr 2 kap. 8 § RF) och
- den personliga integriteten i ideell mening (skyddet för personligheten och för privatlivet inkl. den privata ekonomin, jfr 1 kap. 2 § RF).

Kommittén om ideell skada

Kommittén om ideell skada framhöll i sitt betänkande *Ersättning för kränkning genom brott* (SOU 1992:84) att termen integritet i rättsliga sammanhang från början hade förekommit främst med avseende på sådana bestämmelser som slår vakt om den kroppsliga eller fysiska integriteten, t.ex. straffstadganden om misshandel (s. 187 f.). Med tiden hade termen integritet emellertid kommit att alltmer avse också skyddet för rent immateriella (ideella värden). Till belysning av begreppets numera vidsträckta betydelse i rättsliga sammanhang hänvisade kommittén till Tvångsmedelskommitténs indelning av integritetsbegreppet. Beträffande det immaterialrättsliga skyddet framhöll kommittén att detta skydd avsåg kränkningar i upphovsmannens skapande personlighet sådan den kommit till uttryck i verket.

Kommittén om genetisk integritet

I betänkandet *Genetik, integritet och etik* (SOU 2004:20) konstaterade Kommittén om genetisk integritet att ordet integritet kommer från ett latinskt ord som betyder orörd, hel. Begreppet kunde enligt kommittén delas upp så att man gör en distinktion mellan fysisk och psykisk integritet. När det gäller fysisk integritet är den helhet som avses kroppen. Kravet innebär bl.a. att ingen har rätt att undersöka någon annans kropp utan den andres samtycke. När det gäller mental eller psykiskt integritet, är den helhet som är utgångspunkten det samlade komplexet av individens värderingar,

föreställningar, åsikter och önskningar, liksom individens trosföreställningar och mentala liv. Detta får inte bli föremål för intrång eller manipulation. Individens åsikter eller värderingar skall respekteras – det är själva huvudtanken. Sedan kan detta krav preciseras i olika riktningar och tolkas på flera sätt.

Den personliga integritetens paradox

I artikeln *Staten måste agera på etikens slagfält* (tidskriften Axess, Tema: Genetik och integritet, juni 2005) behandlar fil. dr. Ludvig Beckman den aspekten av den personliga integriteten som har att göra med det privata, det intima och det som är individen fysiskt nära. Han påpekar att det i engelsktalande länder inte talas om ”personal integrity”, men desto mer om ”privacy”. Till exempel är kroppsliga övergrepp att betrakta som en integritetskränkning och inte bara som en möjlig fysisk skada. Ett knytnävsslag i ansiktet är en kränkning, eftersom det utgör ett intrång i den intima och därför den privata sfären. Personlig integritet kan dock enligt Beckman inte likställas med respekten för det privata. Att vara en ”person” är också att vara en individ med förmågan att fatta egna och självständiga beslut. Rätten att bestämma över sig själv är därför ytterligare en viktig aspekt av den personliga integriteten. Det innebär att även obetydliga inskränkningar av det privata upplevs som allvarliga – om de är ofrivilliga. Respekten för den personliga integriteten har alltså två sidor, privatliv och självbestämmande. För att åskådliggöra skillnaden dem emellan återgår Beckman till exemplet knytnävsslaget. Den som väljer att delta i en boxningsmatch kan inte efteråt påstå att han eller hon inte samtyckt till att bli slagen i ansiktet. Det är alltså ingen kränkning av självbestämmandet. Trots det kvarstår kränkningen av det privata. Som ett annat exempel nämner Beckman den ambivalens många erfar inför de desperat självutlämnande ungdomarna i dokusåpor. Dessa deltar ju frivilligt och kränks därför knappast. Å andra sidan är deras personliga integritet inte heller oantastad efter att de själva lämnat ut sig i mer eller mindre intima situationer. Här uppstår enligt Beckman den personliga integritetens paradox. Att värna integriteten med avseende på det privata, exempelvis genom att förbjuda prostitution, kan innebära att integriteten samtidigt inskränks med avseende på självbestämmandet.

2.2.3 Kommitténs utgångspunkt

Kommitténs grundläggande uppgift är enligt direktiven att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten. Någon definition av detta begrepp finns inte i lagstiftningen och har inte heller givits i kommitténs direktiv. Omfattningen av kommitténs arbete kan därför i viss mån sägas bero på vad kommittén själv lägger in i begreppet personlig integritet.

Som framgått av redogörelsen ovan är det inte möjligt eller i varje fall inte för ändamålet meningsfullt att försöka ge en positiv bestämning av den personliga integriteten, dvs. att formulera en beskrivning som pekar ut alla de situationer i vilka individen har rätt att få sin integritet respekterad och skyddad. Det är svårt nog att indirekt bestämma det skyddsvärda området, även om försök i den riktningen har gjorts i form av så kallade kränkningsförteckningar.

Uppgiften att på lämpligt sätt avgränsa kommitténs arbete behöver emellertid i praktiken inte vara så svår som det nyss sagda kan ge intryck av. Det sammantagna intrycket av direktiven, tidigare utredningsarbete och den allmänna diskussion som förts genom åren ger trots allt en ganska bra bild av vad det är som kommittén förväntas undersöka och analysera. Denna bild sammanfaller i stor utsträckning med de områden som undersöktes av 1966 års integritetsskyddskommitté och, om än i blygsammare format, Jermstens 1994 framlagda studie *Skyddet för enskilda personers privatliv* (Ds Ju 1994:51).

Med denna utgångspunkt skulle kartläggningsarbetet begränsas till att i huvudsak avse vad som med en sammanfattande benämning kan kallas den personliga integriteten i ideell mening. Det innebär att kommittén avstår från att djupstudera exempelvis skyddet för äganderätten, för den personliga friheten och rörelsefriheten eller för liv och hälsa. Det innebär också att kommittén inte i alla avseenden detaljgranskar hur Sverige uppfyller sina åtaganden enligt artikel 8 i Europakonventionen; i huvudsak utanför undersökningen faller härigenom straffbestämmelserna vid sexuella och andra kroppsliga övergrepp, frågan huruvida den svenska lagstiftningen i tillräcklig utsträckning medger könsbyte och fastställande av faderskap samt grunderna för omhändertagande av barn och för utlänningars rätt att i vissa fall vistas i landet; i huvudsak utanför undersökningen faller också en lång rad

beteenden som är straffrättsligt sanktionerade av väsentligen andra skäl än hänsynen till den personliga integriteten men som under vissa omständigheter likafullt kan upplevas som integritetskränkande (såsom olika former av frids- och egendomsbrott). Något annat vore också av rent praktiska skäl i det närmaste ogörligt, eftersom ett inträngande studium av integriteten i denna mycket vidsträckta bemärkelse skulle komma att omfatta stora delar av den svenska lagstiftningen som helhet, en gigantisk uppgift som kommittén inte är dimensionerad för, som den inte blivit ålagd att utföra och som den inte heller för egen del finner vara nödvändig för att uppnå ett gott resultat av sitt arbete.

Även med dessa begränsningar måste emellertid kommitténs kartläggning av lagstiftningen på integritetsskyddsområdet bli synnerligen omfattande. Förutom de generella skyddsregler som finns i bl.a. brottsbalken, skadeståndslagen, namnlagen och personuppgiftslagstiftningen måste kartläggningen ta itu med integritetsskyddet på en stor mängd särskilda rättsområden. Som exempel kan nämnas de regelverk som gäller vid respektive i brottsundersökning, författningsskyddad verksamhet, gränskontroll, fiskal och exekutiv verksamhet, kreditupplysning och inkassoverksamhet, hälso- och sjukvård, forskning och statistik, socialtjänst, skola och skolhälsovård, socialförsäkring, arbetslivet, optisk övervakning och hantering av post och elektroniska kommunikationstjänster samt för massmedier och Internet.

Avgränsad på detta sätt skulle det kunna sägas att *informationen om den enskilde* står i blickpunkten för kommitténs undersökning, men att det också är nödvändigt med en kringsyn när det gäller företeelser som på annat sätt är starkt förknippade med den personliga integriteten, såsom användningen av identifieringsdata avseende den enskildes namn, bild och liknande. Mer konkret synes en så avgränsad kartläggningsuppgift ganska väl kunna fångas in med hjälp av följande fyra frågekomplex:

- Hur skyddas enskilda personer mot olovlig insamling av uppgifter om deras privata förhållanden och hur avgränsas ”lovligt” uppgiftsinsamlande (såväl i förhållande till andra enskilda som till det allmänna)?
- Hur skyddas enskilda personer mot olovligt offentliggörande eller annan negativ användning av uppgifter om deras privata förhållanden och hur avgränsas vad som i detta sammanhang är

”lovligt” (såväl i förhållande till andra enskilda som till det allmänna)?

- Hur regleras skyddet mot intrång i någon enskilds privata sfär (såväl fysiskt som i annan mening) där syftet är att inhämta information om den enskilde, och hur avgränsas sådana ”lovliga” intrång (såväl i förhållande till andra enskilda som till det allmänna)?
- Hur skyddas identifieringsdata som namn, bild och liknande?

En gemensam nämnare för tidigare försök att beskriva vad som egentligen avses med personlig integritet kan sägas vara att man har uppfattat integriteten som en ”sfär” som i olika skikt omsluter den enskilde. De yttre skikten rör den enskildes integritet i rent fysisk mening liksom den rumsliga, materiella och kroppsliga integriteten. Dessa yttre skikt inkluderar en mångfald vitt skilda företeelser som onekligen i viss mening är integritetskränkande – fängelsestraff, expropriation, tvång att använda bilbälte etc. – men som i varje fall i den allmänna debatten inte främst brukar förknippas med problemområdet personlig integritet. De innersta skikten, sfärens kärnområden, är däremot intimt förbundna med individen och oupplösligt sammanflätade med dennes personlighet. En avgränsning som tar sin utgångspunkt i informationen om den enskilde och som även befattar sig med användningen av identifieringsdata synes i allt väsentligt fånga in just dessa inre skikt av den personliga integriteten och är därför väl lämpad att användas som huvudsaklig arbetsmetod för kommitténs kartläggning av skyddet för den personliga integriteten.

2.3 Den tekniska utvecklingen[1]

2.3.1 Utvecklingen då och nu

I direktiven till 1966 års integritetsskyddskommitté stod teknikens faror för den personliga integriteten i centrum:

> Som ett resultat av den tekniska utvecklingen har under senare år kommit fram en mångfald nya apparater för ljudöverföring, ljudupptagning och fotografering. Det har bl.a. blivit möjligt att tillverka mikrofoner, radiosändare, bandspelare och kameror i sådant

[1] Framställningen bygger på ett underlag som framtagits av Datainspektionen.

> format att de lätt kan döljas i kläder, tändsticksaskar, pennor eller andra bruksföremål. Vissa apparattyper kan utan svårighet anbringas på väggar och möbler på ett sådant sätt att de lätt undgår upptäckt. Också smygfotografering på stora avstånd är möjlig. - - Denna tekniska utveckling har på flera håll i världen väckt farhågor för missbruk. Även i vårt land har pekats på riskerna för att övervakningsapparater i mikroformat kan komma att finna vägen bl.a. till mindre nogräknade personer som vill använda dem för att utspionera andras privatliv och för att sätta sig i besittning av affärs- eller yrkeshemligheter.

I betänkandet *Skydd mot avlyssning* (SOU 1970:47) försökte 1966 års integritetsskyddskommitté att noggrant beskriva den tidens tekniska apparatur, dess förekomst i Sverige och vilka tekniska skyddsåtgärder som kunde vidtas. På det akustiska området märks rubriker som Mikrofoner, Radiosändare, Trådsändare, Telefoner och Mottagningsapparatur. Motsvarande rubriker på det optiska området upptar exempelvis Miniatyrkameror, teleobjektiv och TV-kameror, Mörkerapparatur och Laserutrustning. Ett kvarts sekel senare konstaterades i studien *Skyddet för enskilda personers privatliv* (Ds 1994:51) att den tekniska utvecklingen var både omfattande och snabb och att det därför inte kunde bli fråga om att inom ramen för studien lämna annat än en mycket översiktlig redogörelse för vad som hänt på området sedan 1966 års kommitté slutför sitt uppdrag. Studien innehåller således ett kortfattat avsnitt om den tekniska utvecklingen, varvid bland annat uppmärksammas möjligheten att avlyssna trådlösa telefoner och mobiltelefoner samt anmärks på säkerhetsbrister beträffande elektronisk post som sänds i ”[s]ystem med yttre anslutning via telenätet”.

Om man i dag, ytterligare tretton år senare, försöker överblicka inte bara dagens teknik utan också hur framtidens teknik kan komma att påverka den personliga integriteten, får man till en början inte glömma bort att all den teknik som i dag finns tillgänglig ännu inte utnyttjas fullt ut. Det finns ingen anledning att anta att de utvecklingstendenser som redan finns, kommer att mattas eller upphöra; kapaciteten för behandling och kommunikation ökar, olika tekniker smälter samman och tillämpningar integreras. I och med den fortsatta utbredningen av trådlösa nätverk där många enheter kommunicerar med varandra, går databehandlingen mot att bli allomfattande, ”ubiquitous computing”. Men det är inte längre själva tekniken som är mest

intressant, utan fokus flyttas till tillämpningarna, som integreras i vardagen.

2.3.2 Två utvecklingslinjer

Från ett integritetsperspektiv kan man urskilja två utvecklingslinjer. Den första är den utveckling som direkt syftar till ökad kontroll, spårbarhet och övervakning av individer; den andra är tekniker som i grunden är harmlösa, men vars tillämpningar kan ge samma effekter som biprodukter.

I den förstnämnda kategorin är ofta drivfjädern att ny teknik ger nya möjligheter att begå straffbara handlingar. Då behöver de brottsbekämpande myndigheterna ta fram nya verktyg. De nya teknikerna kommer i sin tur att användas både av samhället och av enskilda, för att öka säkerheten eller känslan av trygghet.

I den andra kategorin handlar det om att uppgifter som behandlas för ett harmlöst ändamål också kan användas för andra syften som kan vara integritetskänsliga. Sammanställningar av data kan ge upplysningar som ligger långt ifrån behandlingens ursprungliga syfte. Exempel på sådana ändamålsglidningar är samkörningar mellan datasystem eller behandling av elektroniska spår, dvs. data som kan ge upplysningar om någons förehavanden, ofta kopplade till en tidpunkt eller en plats. När vi använder kreditkort lagras uppgifter om när och var kortet har använts, och när vi talar i mobiltelefon genereras uppgifter om vilken basstation som vidarebefordrade samtalet och vid vilken tidpunkt. På samma sätt registreras uppgifter i biltullar, i elektroniska passersystem osv.

2.3.3 Utvecklingen inom vissa teknikområden

Tillämpningar via Internet

Aktiviteter på Internet – e-post, surfning eller fildelning – registreras på olika ställen, till övervägande del helt utanför den enskildes kontroll. Uppgifterna behöver kanske inte var för sig utgöra ett hot mot den privata sfären, men sammantagna kan de ge en mycket detaljerad bild av den enskildes vardagsliv. Om behandlingen utförs på ett kvalificerat sätt och i syfte att kartlägga en viss individs förehavanden kan effekterna bli förödande för den personliga integriteten. Det spelar härvid i princip ingen roll om

behandlingen utförs av en privatperson i eget intresse eller i behörig ordning av en statlig myndighet.

Internet fortsätter att växa, inte bara med avseende på antalet uppkopplade enheter utan också på antalet tillämpningar. Allt större del av vår kommunikation passerar vid ett eller annat tillfälle över Internet. Oskyddad kommunikation kan inte bara avlyssnas, den kan också sparas vid så kallade noder som passeras på vägen. Den som publicerar något på Internet eller oskyddat kommunicerar över nätet, avhänder sig i viss mån kontrollen över informationen. Det är inte möjligt att förutse vem som kommer att behandla informationen eller i vilka syften. Detta ställer höga krav på säkerheten i system som är kopplade till Internet, särskilt om de innehåller känsliga personuppgifter.

Det finns tekniker som används av sökmotorer på Internet för att strukturera och indexera publicerad information, och de teknikerna förfinas fortlöpande. Ursprungsidén var att den sökande snabbt skulle hitta den informationen som var mest relevant i förhållande till hans fråga. Sökteknikerna utvecklar ständigt nya metoder för att kvantifiera relevans, dvs. räkna ut vad som egentligen efterfrågas vid en viss sökning. Informationen som dessa beräkningar bygger på ger samtidigt kunskap om vad användarna intresserar sig för, något som utnyttjas inom bland annat reklambranschen. Det största kommersiella intresset för sökningstekniken är i dag knutet till leverans av riktade annonser, vilket har medfört att sökmotorerna i dag omsätter miljarder dollar årligen. Fenomenet utgör ett klart exempel på ändamålsglidning. *Google*, det numera dominerande företaget i branschen, har enligt egna uppgifter aldrig raderat några uppgifter om gjorda sökningar. Tekniskt sett finns inget som hindrar att denna enorma mängd sparade data används för andra syften än de ursprungliga. En särskild tjänst som *Google* har utvecklat och tillhandahåller är att ta fram information som inte längre finns tillgänglig på Internet, men som finns lagrad i företagets databaser. I den mån denna information är felaktig eller missvisande är möjligheterna att rätta uppgifterna i praktiken obefintliga. Den aktuella tjänsten får härigenom en konserverande effekt, vilket i sig utgör en fara för den personliga integriteteten.

De vanliga sökmotorerna – *Google*, *AlltheWeb*, *Yahoo*, *Altavista* m.fl. – samlar in och behandlar alla uppgifter som är publicerade på Internet. Det finns emellertid inga hinder att utveckla söktjänster som även samlar in uppgifter utifrån särskilda kriterier eller från

specificerade källor som e-handelsplatser eller ”communities” där människor med gemensamma intressen kommunicerar.

Söka och sammanställa information

Att söka eller sammanställa information ur stora datamängder utifrån givna kriterier har varit möjligt länge. På så sätt kan man framställa information som inte var tillgänglig före sammanställningen (och som då utgjorde vad som ofta benämns potentiella handlingar). Tekniken kan användas för att kontrollera eventuella samband mellan olika specificerade data. Ett steg längre går s.k. *datamining*, där man använder matematisk statistik, maskininlärning och mönsterigenkänning för att hitta samband mellan data som till synes är helt oberoende av varandra. Eftersom dessa data samverkar slumpmässigt kommer också en mängd falska samband att kunna påvisas (såsom att fluktuationerna i bomullspriset visar likhet med AIK:s formkurva).

De angivna teknikerna har med framgång använts i kommersiella syften, vilket ingett förhoppningar om att kunna använda dem även för att motverka terrorism och för andra brottsbekämpande ändamål. Användning av sådana metoder utan klar insikt om teknikens inneboende begränsningar innebär stora hot mot den personliga integriteten. Det gäller i synnerhet om tekniken kopplas till automatiserade beslut där den enskilde inte kan kontrollera underlaget för beslutet. Om tvist skulle uppkomma om beslutets riktighet, finns dessutom all bevisning hos den ena parten.

Möjligheter till censur och filtrering

En effekt av att allt större del av vår kommunikation är digitaliserad, är att möjligheterna till censur och filtrering har ökat. Den som kontrollerar en nod där datatrafik passerar, kan sätta upp spärrar för att förhindra viss kommunikation. Tekniken i dessa passiva spärrar har hittills inte varit särskilt avancerad och har kunnat kringgås med enkla medel, men i takt med att spärrteknikerna utvecklas ökar riskerna för den personliga integriteten. Filtrering är exempel på en mer aktiv åtgärd som kräver att innehållet i kommunikationen analyseras i realtid vid noden. I dag saknas den beräkningskapacitet som krävs för att använda filtrering

i stor skala, men tekniken kan tillämpas på avgränsade områden. Dessa filter kräver att kommunikationen sker i klartext eller att den går att dekryptera. Det innebär att den som kontrollerar noden får tillgång till information, som naturligtvis kan vara av integritetskänslig karaktär.

Ett annat sätt att kontrollera digitaliserad kommunikation är att i efterhand analysera lagrade trafikdata. Ingrepp i själva kommunikationen är då inte möjlig, men det går att rekonstruera kommunikationsvägar och kartlägga kommunikationsmönster. Beroende på vilka trafikdata som lagras kan de användas för att kontrollera vem som har kommunicerat med vem och på vilket sätt. Lagring av trafikdata kan också användas för att binda en person till en viss plats vid en viss tidpunkt. I EU:s medlemsländer kommer obligatorisk lagring av trafikdata att inom kort genomföras i stor skala som följd av ett EG-direktiv våren 2006.

Användningen och utvecklingen av system för DRM (Digital Rights Management) har kommit till för att ge rättighetsinnehavare möjlighet att förhindra att upphovsrättsskyddat material används på annat sätt än de själva har godkänt. Dessa system ger också upplysningar om den enskildes mediekonsumtion och kan användas för att göra profiler eller kartlägga smak och vanor. Bredbandsdistribution ger samma möjligheter eftersom distributionen i sig ger upphov till elektroniska spår i form av trafikdata och loggar. Designen av dessa system kan komma att utvecklas så att anonym konsumtion av upphovsrättsskyddat material omöjliggörs och gå i riktning mot en generell övervakning av all information som den enskilde tar del av. Särskilt snabbt kan denna utveckling gå om funktionen kopplas ihop med operativsystem och hårdvara. En utveckling i denna riktning har de facto redan inletts.

Kartläggning av kommunikationsvägar

Möjligheten och intresset för att kartlägga individers kommunikation har givit upphov till motreaktioner. Särskilt märks en ökad efterfrågan på tjänster som på olika sätt tillåter användarna att uppträda under falsk identitet eller anonymt. På grund av Internets grundläggande konstruktion och de trafikdata som genereras, är det emellertid svårare att dölja än att säkerställa en identitet. Det förhållandet att det har visat sig svårt att juridiskt binda en person vid en viss elektronisk kommunikation, minskar inte nämnvärt

riskerna för den personliga integriteten. Redan det faktum att en person med stor sannolikhet kan kopplas till vissa data kan innebära en integritetskränkning.

Det ökade intresset för kartläggning av kommunikationsvägar inskränker sig inte till elektronisk kommunikation. System som kartlägger rent fysiska kommunikationer tilldrar sig allt större intresse från trafikföretag, arbetsgivare, försäkringsbolag och statliga organ. Motiven varierar och omfattar allt från miljöhänsyn och stads- eller arbetsplanering till effektiviseringar och terroristbekämpning. Elektroniska färdbevis har tagits i bruk som ger resenärerna tillgång till olika tjänster och nyttigheter, såsom avgifter baserade på färdsträcka och kompensation vid förseningar. Trafikdata från mobiltelenäten används redan i dag för att leverera tjänster för positionsbestämning, och s.k. svarta lådor i fordon har länge använts för att analysera eventuella konstruktionsbrister vid olyckor. Med utvecklad teknik är det möjligt att i detalj registrera fordons förflyttningar, förarens körstil och varjehanda händelser, något som i sin tur möjliggör sådant som automatiserade beslut om vägtrafikavgifter, fortkörningsböter och differentierade försäkringspremier. Alla dessa detaljerade sammanställningar över individernas förflyttningar, och eventuellt också vanor och personligheter, innebär samtidigt nya risker för den personliga integriteten.

Lagringskapaciteten ökar

Det har blivit vanligt att flyttbara elektroniska enheter förses med digitala minnen. Kameror, mobiltelefoner, mediespelare, handdatorer, hårddiskar och USB-minnen har mycket stor lagringskapacitet, vilket naturligtvis ökar risken för spridning av personuppgifter till obehöriga och även risken för otillåten behandling av uppgifterna. En för den personliga integriteten väl så stor risk är att skadlig eller på annat sätt oönskad programvara sprids i organisationers nätverk eller mellan privata datorer.

Automatiserad identifiering

Intresset av att identifiera personer och av att kunna verifiera en uppgiven identitet (s.k. autentisering) har ökat. Motivet är som regel ett behov av ökad säkerhet. Utvecklingen går allt mer mot automatiserad identifiering, exempelvis med hjälp av system som är kopplade till digitala övervakningskameror och användning av s.k. RFID-kretsar. När personer identifieras, kopplas de samtidigt till en viss plats eller handling vid en viss tid. Det medför risker för den personliga integriteten, särskilt i fall då identifiering och verifiering tillgrips utan godtagbara skäl.

Biometriska uppgifter har direkt koppling till fysiska personer eftersom de baseras på enskildas egenskaper eller beteenden. Rätt använda kan uppgifterna stärka rättssäkerheten och den personliga integriteten, eftersom säkrare identifiering kan minska risken för identitetsstöld och bedrägerier. En alltför stark tillit till metodens tillförlitlighet kan emellertid även locka till bedrägeriförsök, som kan få svåra konsekvenser om de lyckas. Biometri kan också användas för att negativt fastställa en identitet, något som kan användas för att fria oskyldigt misstänkta eller för att hindra personer från att begagna flera identiteter. Ett noggrant och säkert registreringsförfarande är av stor vikt, eftersom hela syftet med systemet förfelas om en person registreras under oriktig identitet.

Alla biometriska metoder kan innefatta två typer av fel: Systemet kan godkänna fel person (”false positives”) eller vägra godkänna rätt person (”false negatives”). I båda fallen kan konsekvenserna bli förödande för den enskilde, som dessutom sällan eller aldrig ges möjlighet att kontrollera om uppgifterna är riktiga eller att metoden är tillförlitlig. Från integritetsskyddssynpunkt bör det därför ställas höga säkerhetskrav på systemet och dess data. Det är viktigt att riskerna uppmärksammas redan från början, eftersom det är svårt att i efterhand säkra eller komma till rätta med brister i behandlingen. När biometriska data lagras digitalt ökar också risken för att de sprids och behandlas utom personens kontroll, i synnerhet när det gäller system där de biometriska uppgifterna registreras utan personens medverkan.

Elektronisk administration innebär risk för identitetsstöld

Riskerna för identitetsstöld ökar i takt med att allt fler officialhandlingar kan utföras och juridiskt avtal kan ingås elektroniskt. Utvecklingen av den s.k. e- eller 24-timmarsmyndigheten har inte tillkommit bara för att erbjuda medborgarna nya sätt att kommunicera med myndigheterna eller för att ge myndigheterna bättre möjligheter att kommunicera med varandra. Avsikten har också varit att ärenden som involverar flera myndigheter skall kunna handläggas effektivare med hjälp av gemensamma eller sammankopplade ärendehanteringssystem. Detta innebär med nödvändighet att fler personer bereds tillgång till fler uppgifter om fler medborgare. Från integritetsskyddssynpunkt är det därför viktigt att definiera ansvaret vid behandlingar som omfattar flera huvudmän. I system där känsliga personuppgifter behandlas blir frågor om behörighetskontroll och behandlingshistorik särskilt viktiga.

Tekniker för att underlätta identitetsstöld, exempelvis genom att lura av personer deras autentiseringsuppgifter (s.k. Phishing), blir allt mer avancerade. Denna utveckling kan förväntas fortsätta. Även spionprogram och övervakningsprogram för installation på enskilda datorer i syfte att registrera användarens aktiviteter blir allt mer sofistikerade. Intresset är stort från så vitt skilda grupper som oroliga föräldrar eller äkta hälfter, skolor, arbetsgivare och kriminella. I betänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38) har föreslagits att tekniken även skall få tas i anspråk i brottsbekämpande syfte. Genom att inkludera s.k. rootkits kan spionprogrammen göras osynliga, både för användare och operativsystem. Omfattande åtgärder krävs för att därefter upptäcka dem. Programmen kan också riktas in på ren övervakning. En s.k. keylogger kan redan med hjälp av äldre teknik användas för att spela in alla tangentbordsnedtryckningar, men ett spionprogram kan registrera enbart önskade uppgifter, såsom chattkonversationer, användarnamn och lösenord för vissa tjänster. Programmen kan installeras på plats eller spridas i form av virus eller trojaner, utan att det krävs fysisk tillgång till den övervakande datorn.

2.3.4 Vilket betraktelsesätt bör användas på ny teknik?

När man diskuterar teknikens inverkan på den personliga integriteten har man traditionellt betraktat en viss teknik som ett hot med åtföljande risker. Den personliga integriteten blir då ett skyddsobjekt som man kan behöva skydda med hjälp av lämpliga åtgärder. Detta betraktelsesätt kan vara ändamålsenligt i fråga om teknik som direkt syftar till ökad kontroll, spårbarhet och övervakning, trots att man då samtidigt riskerar att förbise teknikens eventuella positiva effekter på integritetsskyddet. Ett annat betraktelsesätt är att uppfatta tekniken som något som används i ett visst syfte. Vad som då blir angeläget från integritetsskyddssynpunkt är att först bedöma den aktuella åtgärdens verkan i förhållande till syftet, och därefter väga konsekvenserna av åtgärden mot den enskildes rätt till personlig integritet. Svårigheterna med detta betraktelsesätt är desamma som vid annan intresseavvägning, men fördelen är att tekniker som sekundärt påverkar den personliga integriteten kan värderas på ett mer ändamålsenligt sätt.

2.3.5 Aktuella utvecklingstendenser i sammanfattning

Inom Datainspektionen har följande tendenser inom teknikutvecklingen utpekats som särskilt relevanta för inspektionens verksamhet år 2007.

1. Det finns en tendens att i allt högre utsträckning vilja identifiera människor. Användningen av biometri i detta syfte börjar ta fart och inkluderas i pass och andra id-handlingar.
2. En utredning pågår om hur trafikdatalagringsdirektivet skall genomföras i svensk lagstiftning. Elektroniska spår som lämnas i samband med elektronisk kommunikation, t.ex. telefonsamtal, e-post och Internetanvändning skall sparas och användas för att i efterhand göra det möjligt att utreda mellan vilka kommunikation ägt rum.
3. Internationaliseringen innebär att personuppgifter sprids utanför Sverige. Multinationella bolag vill exempelvis överföra och samla personuppgifter centralt i organisationen.
4. Det internationella tull- och polissamarbetet medför krav på ökat utbyte av personuppgifter.

5. RFID (Radio Frequency Identification) används för identifiering av personer och olika typer av betaltjänster, t.ex. inom kollektivtrafiken.
6. Fortsatt ökad användning av bevakningskameror på arbetsplatser, i hyreshus och i skolor. Kameror som klarar av att känna igen ansikten och fånga upp misstänka rörelsemönster utvecklas.
7. Förbättrade söktjänster för sammanställning av ostrukturerade data fortsätter att utvecklas, liksom möjligheten att utföra sökningar i stora informationsmängder.
8. IT byggs in i och samspelar med annan teknik. I bilar testas system som kommunicerar och samverkar med system utanför bilarna, t.ex. larmsystem, räddningstjänst och satellitpositioneringssystem.
9. Arbetet fortskrider med att förverkliga visionerna om 24-timmarsmyndigheten och en sammanhållen e-förvaltning.
10. Arbetet kring sammanhållna journaler och ökat utbyte av patientuppgifter mellan olika typer av vårdgivare fortsätter. Kommuner kopplas ihop med sjukvårdsnäten.
11. Program som innehåller funktioner för att samla information om användaren blir vanligare (s.k. spyware). Även aktiva eller riktade försök att komma åt sådan information ökar (s.k. phishing).
12. Kommunikationskapaciteten genom bredband och tredje generationens mobilsystem (3G) ökar liksom användningen av trådlösa nät, t.ex. WLAN, i hemmet, på allmänna platser och på arbetsplatser.
13. IT och telekommunikationstekniken växer samman. Mobiltelefoner kan mer och mer ses som datorer med omfattande lagrings- och multimediakapacitet. Stora mängder trafikdata i teletrafiken skapas och registreras.
14. Portabla enheter (t.ex. digitalkameror, mp3-spelare, portabla hårddiskar, USB-minnen, handdatorer och mobiltelefoner) får allt större datalagringskapacitet.
15. Kreditupplysningsjänster via SMS och på Internet fortsätter att utvecklas.

16. Uppgifter som tidigare utfördes på den egna datorn, t.ex. ordbehandling, planeringskalendrar och liknande, kan utföras med hjälp av webbtjänster.
17. Anonymiseringstjänster för Internet fortsätter att utvecklas och får ökad spridning.

3 Kommitténs attitydundersökning i sammandrag

På uppdrag av Integritetsskyddskommittén genomförde Statistiska centralbyrån (SCB) under tiden september–december 2006 en enkätundersökning. Syftet med undersökningen var att få en ungefärlig uppfattning om allmänhetens inställning till behovet av skydd för den personliga integriteten, särskilt när detta behov kommer i konflikt med andra behjärtansvärda intressen. Enkäten besvarades av drygt 1 000 slumpvis utvalda personer av den svenska befolkningen i åldern 18–79 år och omfattade 78 frågor som hade utformats av kommitténs sekretariat under medverkan av SCB och Institutet för rättsinformatik vid Stockholms universitet. Svaren redovisas uppdelat på fyra åldersgrupper och två utbildningsnivåer. Utfallet av enkäten redovisas fullständigt i *bilaga 4* samt i vissa delar och i förenklad form här nedan.

Beträffande användningen av *personnummer* ansåg en majoritet (66 %) att dagens nivå är lagom. För tretton år sedan ställde Personnummerutredningen i en motsvarande enkät frågan om hur stor minskning av servicegraden (exempelvis i form av att den enskilde tvingades anmäla adressändringar på flera olika ställen) som urvalspersonerna kunde acceptera för att uppnå en begränsning av personnummeranvändningen. Då svarade 24 procent att de inte kunde acceptera *någon* minskning av servicegraden (se betänkandet *Personnummer – Integritet och effektivitet*, SOU 1994:63). Exakt samma fråga ställdes i den nu aktuella enkätundersökningen, varvid 48 procent sade sig inte kunna acceptera en sänkt servicenivå.

En stor majoritet (77 %) ansåg att det var acceptabelt att oskyldiga personers integritet kränks vid *brottsutredningar*, t.ex. genom telefonavlyssning. Inte mer än 10 procent var helt emot användning av mycket integritetskränkande metoder, såsom buggning och hemlig avläsning av datorer. Inom den yngsta ålderskategorin (18–32 år) var dock en större andel, 19 procent,

helt emot sådana metoder. Det kan noteras att sistnämnda fråga gällde integritetskränkande metoder som i dag inte är tillåtna i polisarbetet, ändå ville 87 procent inte utesluta att metoderna skulle få användas.

När det gäller att komma åt *terrorism och annan grov brottslighet* ansåg en stor majoritet (79 %) att kontrollen över medborgarna bör öka. Bara 2 procent ansåg att kontrollen bör minska. Motsvarande andel var för *skattebedrägeri* 3 procent, för *bidragsfusk* 2 procent och för *fortkörning* 17 procent.

Enkätsvaren gav vid handen en starkt positiv inställning till *kameraövervakning* i syfte att minska brottsligheten. Det gällde även när syftet är att förhindra eller avslöja förhållandevis mindre allvarlig brottslighet som klotter, skadegörelse och snatteri. En mycket stor majoritet (90 %) accepterade kameraövervakning också när det behövs för att folk skall känna sig tryggare.

När det särskilt gällde risken för *flygplansterrorism* ansåg 93 procent att inskränkningar i integritetsskyddet och bekvämligheten är motiverade. I åldersgrupperna 33–48 och 49–64 år ansåg 46 procent att *stora* inskränkningar var motiverade medan en betydligt lägre andel, 21 procent, i den yngsta ålderskategorin ansåg det.

DNA-registrering uppfattade 48 procent som känslig från integritetsskyddssynpunkt, medan 38 procent ansåg att DNA-registrering inte var det. En mycket stor majoritet ansåg att personer som är misstänkta för brott precis som i dag bör DNA-registreras. Påståendet ”*Även om många människor upplever det som integritetskränkande bör hela befolkningen DNA-registreras*” höll 51 procent med om medan 34 procent svarade att de inte höll med.

Bland en rad frågesvar på *skolans* och *arbetslivets* områden kan noteras att 86 procent ansåg att det är godtagbart från integritetsskyddssynpunkt att lärare tar kontakt med föräldrar om elevers uppförande utan att eleverna vet om det. Beträffande alkohol- och drogtester av personal på arbetsplatser ansåg 83 procent att arbetsgivare när problem uppstår bör utreda, informera och diskutera med personalen. Betydligt färre, 31 procent, ansåg att arbetsgivaren bör uppmana hela eller delar av personalen att genomgå alkohol- och drogkontroll.

Enkäten upptar även ett antal frågor av *pressetisk* karaktär. På frågan om tidningar och TV bör publicera namn och bild på farliga mördare och sexualförbrytare som har rymt från fängelser eller psykvårdsanstalter, svarade 73 procent ”Ja, så att andra personer

varnas och tar sig i akt", medan 7 procent – 12 procent i den mer högutbildade gruppen – svarade "Nej, även grova brottslingar har rätt till personlig integritet". En klar majoritet tyckte att kändisjournalistiken har blivit för närgången. 79 procent ansåg att det behövs strängare regler om skadestånd till människor som behandlas illa av medierna. En stor majoritet, 82 procent, ansåg även att staten har en skyldighet att genom lagstiftning och förbud ingripa mot integritetshoten på *Internet*. Bara 5 procent ansåg att staten inte har en sådan skyldighet.

Fler (49 %) var för än mot (34 %) att alla uppgifter om e-posttrafik lagras så att myndigheterna i brottsutredande syfte kan gå in och kontrollera i efterhand. I den yngsta åldersgruppen var ungefär lika många för som mot, medan 57 procent i den äldsta gruppen, 65–79 år, var för och 16 procent mot. Frågan var delvis föranledd av EU:s år 2006 antagna direktiv om *obligatorisk lagring av teletrafikdata*.

Att företag och privatpersoner kränker andra människors integritet genom *kartläggning av köpvanor* ansåg 70 procent. En ännu större andel, 85 procent, ansåg att företag och privatpersoner kränker andras integritet *genom påträngande marknadsföring*. Bara 19 procent hade emellertid själva upplevt att deras eller deras familjs integritet hade kränkts av företag eller privatpersoner. 49 procent ansåg att det är integritetskränkande att behöva lämna elektroniska spår, men bara 10 procent – 6 procent i den yngsta kategorin och 16 procent i den äldsta – avstod av den anledningen så långt möjligt att lämna sådana spår.

Toleransen för att bli filmad i en bostad av *privata övervakningskameror* som satts upp till skydd mot inbrott var mycket stor. (Av enkätpersonerna svarade dock 8 procent att detta var så obehagligt att de i fortsättningen inte skulle besöka en bostad där de hade blivit filmade). Å andra sidan ansåg 72 procent att det bör krävas medgivande för att få *fotografera* eller *spela in* en annan person. Något krav på medgivande finns som bekant inte i gällande lag.

Uppfattningen att uppgifter av vissa angivna slag i myndigheternas register var *mycket eller ganska känsliga* fördelades enligt följande:

Familjemedlemmar	20 %
Mobiltelefonnummer	21 %
Medlemskap i fackförening, A-kassa och bostadsbidrag	alla 24 %
Betyg	39 %
Tillgångar och skulder	48 %
”Att du har blivit polisanmäld”	56 %
Hälsotillstånd	59 %
”Vilka webbsidor som du har besökt när du surfat på nätet”	61 %
Vem som har talat med vem på telefon	63 %

Beträffande *känsliga personuppgifter* som samlas in av myndigheterna tyckte 59 procent att redan det förhållandet att den insamlande myndighetens personal kan ta del av uppgifterna är *mycket integritetskränkande.* Å andra sidan menade 76 procent att problemet inte är att uppgifterna samlas in och förvaras hos en myndighet utan att det alltför ofta händer att obehöriga personer kommer över uppgifterna, dvs. att registren läcker.

Enkäten upptog inte några frågor på *sjukvårds- och patientsäkerhetsområdet*, främst beroende på att Patientdata-utredningen hösten 2005 lät genomföra en undersökning på det området, vilken finns redovisad i betänkandet *Patientdatalag* (SOU 2006:82). Enligt den undersökningen var 79 procent positiva till att det skapas en enda elektronisk journal för varje patient. Av dessa såg 51 procent inga nackdelar med en sådan journal, medan 28 procent av de positiva kände en viss oro för att obehörig vårdpersonal skulle kunna få tillgång till deras journaluppgifter. När det gällde vilket inflytande en patient skall ha när vårdpersonalen vill läsa patientens journal ansåg 31 procent att patienten, utom i akutsituationer, alltid måste ha lämnat sitt samtycke. Endast 11 procent ansåg att patienten inte skall ha något inflytande över vem som skall få läsa journalen. 71 procent ville kunna ta del av sin patientjournal via Internet. 63 procent var positiva till att uppgifter i patientjournaler används som underlag för forskning.

Kartläggningen

4 Generella skyddsregler i vanlig lag

4.1 Inledning

I förevarande avsnitt redogörs för regler i vanlig lag som syftar till att skydda den personliga integriteten i mer generell bemärkelse och alltså inte endast inom ett visst område. Till dessa regler hör brottsbalkens (BrB:s) bestämmelser om fridsbrott, ärekränkning och brott mot tystnadsplikt samt vissa bestämmelser som kan grunda rätt till skadestånd vid kränkningar av den personliga integriteten. Även frågan om det allmännas skadeståndsansvar i framtiden berörs i detta avsnitt. Generellt verkande regler finns också i lagen (1978:800) om rätten till namn och bild i reklam och i namnlagen (1982:670), som båda reglerar rättsförhållanden mellan enskilda. I detta sammanhang redovisas också de relativt nya reglerna om sekretesskydd för uppgifter i offentliga register. Avsnittet avslutas med en genomgång av generellt tillämpliga EG-rättsliga respektive svenska bestämmelser om skydd för personuppgifter i samband med framför allt automatiserad databehandling.

De här redovisade reglerna kan sägas väsentligen ge uttryck för mer allmänna rättsprinciper som rör rätten till frid, rätten till ersättning för kränkning och rätten till det egna namnet. Till denna kategori kan också, med tanke på informationsteknikens stora utbredning i dagens samhälle, räknas skyddet för personuppgifter.

Redovisningen av de generella skyddsreglerna tjänar sin plats i inledningen av redogörelsen för kartläggningen, eftersom den kan sägas utgöra en nödvändig bakgrundsbild till de särskilda skyddsregler som finns inom respektive område. Någon analys av integritetsskyddets tillräcklighet inom dessa centrala områden görs emellertid inte i detta sammanhang. En sådan analys är av grundläggande betydelse som underlag för kommitténs överväganden om det, vid sidan av befintlig lagstiftning, behövs generellt tillämpliga bestämmelser till skydd för den personliga

integriteten, vilken kommittén återkommer till i sitt slutbetänkande. Analysen av om skyddet för den personliga integriteten är tillfredsställande reglerat inom de centrala rättsområdena redovisas därför i det betänkandet.

4.2 Straffbestämmelser till skydd mot kränkning av den enskildes integritet

4.2.1 Brott mot frihet och frid

I 4 kap. BrB om brott mot frihet och frid finns flera bestämmelser av intresse från integritetsskyddssynpunkt. Det rör sig om regler som framför allt syftar till att ge skydd mot fridskränkningar.

Bestämmelser om *hemfridsbrott* och *olaga intrång* finns i 4 kap 6 §. Med hemfridsbrott avses att någon olovligen tränger sig in eller stannar kvar där annan har sin bostad. Olaga intrång är subsidiärt till hemfridsbrott och har ett annat skyddsområde. Med olaga intrång avses ett olovligt intrång eller kvarstannande i kontor, fabrik, annan byggnad eller fartyg, på upptagsplats eller på annat liknande ställe. Straffet för hemfridsbrott och olaga intrång är i normalfallet böter. Om brottet är grovt döms till fängelse i högst två år.

För *ofredande* (4 kap. 7 §) döms den som handgripligen antastar eller genom skottlossning, stenkastning, oljud eller annat hänsynslöst beteende ofredar någon annan. Som exempel på den första formen av ofredande – att handgripligen antasta annan – kan nämnas att någon uppsåtligen knuffar, tillfälligt håller fast eller spottar på någon annan. Den andra formen av ofredande är att någon genom hänsynslöst beteende ofredar någon annan. För att gärningen skall vara brottslig måste den innebära en kännbar fridskränkning – den utsatte måste verkligen ha blivit störd – och dessutom kunna sägas vara uttryck för hänsynslöshet (Jareborg, *Brotten I – Grundbegrepp: Brotten mot person*, s. 280). Upprepade telefonpåringningar eller liknande trakasserier kan vara straffbara såsom ofredande liksom att kasta sten eller bulta på annans hus eller föra oväsen utanför någons bostad. Kriminaliseringen av ofredande utgör således vid sidan av kriminaliseringen av hemfridsbrott ett skydd för bostadsfriden. Straffet för ofredande är böter eller fängelse i högst ett år.

Enligt 4 kap. 8 § döms den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande, för *brytande av post- eller telehemlighet* till böter eller fängelse i högst två år. Skyddet gäller bara under den tid som meddelandet är under befordran. Brottet brytande av posthemlighet förutsätter inte att den som berett sig tillgång till försändelsen också har läst försändelsen. Att bereda sig tillgång till ett telemeddelande kan ske på liknande sätt som när man bereder sig tillgång till en postförsändelse. Detta gäller t.ex. utskrift av ett telegram eller annat telemeddelande. Meddelande i rundradio faller dock helt utanför bestämmelsen.

Även utan samtycke kan det under vissa förhållanden vara lovligt såväl för post- som telebefordringsföretag att bereda sig tillgång till ett meddelande. För en närmare redogörelse avseende dessa fall, se kapitel 15.

Intrång i förvar utgör subsidiärt brott till brottet brytande av post- eller telehemlighet (4 kap. 9 §). Det innefattar i första hand att man, utan att det är fråga om något som är under befordran, olovligen bryter brev eller telegram (t.ex. efter det att post- eller telebefordringsföretagets befattning med meddelandet upphört). Brottsbeskrivningen är emellertid mycket generell och täcker också in situationen att någon i annat fall bereder sig tillgång till något som förvaras förseglat eller under lås eller på annat sätt tillslutet. Även annat än meddelanden skyddas alltså, men av sammanhanget torde framgå att objektet måste vara en sak som förmedlar ett föreställningsinnehåll (Jareborg, a.a., s. 283). En handling, som ligger på ett bord eller i en olåst låda, skyddas bara om den ändå kan anses vara tillsluten, t.ex. om den förvaras i ett förseglat kuvert eller om dörren till lokalen är låst. Straffet för intrång i förvar är böter eller fängelse i högst två år.

Reglerna i 4 kap. 8–9 §§ ger uttryck för tanken att den enskilde har ett berättigat anspråk på att privata förhållanden inte skall komma till utomståendes kännedom utan hans eller hennes vetskap. Samma tanke ligger bakom bestämmelserna i 9 a § om *olovlig avlyssning*, dvs. vad som i dagligt tal även kallas buggning. Dessa bestämmelser infördes år 1975 på grundval av förslag från 1966 års integritetsskyddskommitté i syfte att effektivisera skyddet på personrättens område mot bakgrund av den tekniska utvecklingen. För olovlig avlyssning kan den dömas som i annat fall än som sägs i 8 § olovligen med tekniskt hjälpmedel för återgivning av

ljud, i hemlighet avlyssnar eller upptar tal i enrum, i samtal mellan andra eller i förhandlingar vid sammanträde eller annan sammankomst, vartill allmänheten inte äger tillträde och som han själv inte deltar i eller som han obehörigen berett sig tillträde till. Det är således inte straffbart att använda sig av på den egna kroppen placerade mikrofoner till att spela in ett samtal som man själv deltar i. Påföljden för olovlig avlyssning är böter eller fängelse i högst två år. Bestämmelsen i 4 kap. 9 a § omfattar inte radiobefordrade meddelanden.

Om någon anbringar tekniskt hjälpmedel med uppsåt att bryta telehemlighet eller att utföra olovlig avlyssning, döms enligt 9 b § för förberedelse till sådant brott. Också i detta fall är påföljden böter eller fängelse i högst två år.

Den som i annat fall än de som träffas av bestämmelserna om brytande av telehemlighet eller olovlig avlyssning utan lov bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för *dataintrång* (4 kap. 9 c §). Påföljden för brottet är böter eller fängelse i högst två år.

4.2.2 Ärekränkning

Reglerna om ärekränkning i 5 kap. BrB är uppdelade på två olika brottstyper; förtal och förolämpning. Kränkning av en persons ära i objektiv mening, dvs. av den aktning eller det anseende som en person åtnjuter bland sina medmänniskor, faller under förtalsbrottet (5 kap. 1 och 2 §§). Även kränkning av en avliden persons ära utgör förtalsbrott (5 kap. 4 §). Kränkningar av en persons ära i subjektiv mening, dvs. av hans egen känsla av att vara aktad eller ansedd, omfattas av kriminaliseringen av förolämpning (5 kap. 3 §).

Enligt 5 kap. 1 § döms den som utpekar någon som brottslig eller klandervärd i sitt levnadssätt eller eljest lämnar uppgift som är ägnad att utsätta denne för andras missaktning, för *förtal* till böter.

Brottet utgör således ett angrepp på någons anseende, hans ”goda namn och rykte”. För att ett förtalsbrott skall föreligga måste gärningsmannen rikta sina förgripligheter till någon annan än den angripne (Jareborg, a.a., s. 291 f.).

Gärningsmannens skall inte dömas till ansvar om han var skyldig att uttala sig eller det annars med hänsyn till omständigheterna var försvarligt att lämna uppgift i saken, förutsatt att han kan visa att

uppgiften var sann eller att han hade skälig grund för den. I frågan om när det sålunda kan vara försvarligt att lämna ärekränkande uppgifter anförde föredragande departementschefen bl.a. följande vid BrB:s tillkomst (prop. 1962:10, s. B 144):

> I den offentliga diskussionen, såväl i tal som i skrift, upprätthålles i vårt land en vidsträckt yttrandefrihet. Denna yttrandefrihet är grundvalen för ett demokratiskt samhällsskick. Det måste finnas utrymme för den politiska debatten, liksom också andra samhälleliga, kulturella och vetenskapliga frågor måste få ventileras, även om därigenom enskilda personer skulle i viss mån angripas. Ett annat viktigt område, där yttrandefriheten bör särskilt beaktas, är den yrkesmässiga nyhetsförmedlingen - - - Avgivandet av tjänstevitsord, vare sig i enskild eller allmän tjänst, är en vanlig situation, där konflikt mellan olika intressen kan uppkomma. Även i övrigt torde uppgifter som lämnas för att tillgodose ett berättigat allmänt eller enskilt intresse få anses lämnade i en på samma sätt privilegierad situation.

Bortsett från de situationer då det alltså är försvarligt att lämna en nedsättande uppgift har det i princip ingen betydelse om uppgiften är sann eller inte. I förtalsmål gäller därför som huvudregel att sanningsbevisning inte är tillåten.

För *grovt förtal* döms enligt 5 kap. 2 § till böter eller fängelse i högst två år. Vid bedömningen av om brottet är grovt skall särskilt beaktas om uppgiften genom sitt innehåll eller den omfattning i vilken den blivit spridd eller eljest var ägnad att medföra allvarlig skada.

Brottet *förtal av avliden* (5 kap. 4 §) förutsätter att rekvisiten för förtal enligt 5 kap. 1 § eller 2 § är uppfyllda. Därutöver krävs att gärningen är sårande för de efterlevande eller den eljest, särskilt med beaktande av den tid som förflutit sedan den förtalade dog, kan anses kränka den frid som bör tillkomma denne.

Enligt 5 kap. 3 § skall den som smädar annan genom kränkande tillmäle eller beskyllning eller genom annat skymfligt beteende mot honom dömas, om gärningen inte utgör förtalsbrott och därmed är belagd med straff enligt 1 och 2 §§, för *förolämpning* till böter. Om brottet är grovt, döms till böter eller fängelse i högst sex månader.

Förolämpning är en fridskränkning i form av angrepp på den utsattes självkänsla. Angreppet måste riktas direkt mot den det gäller. Om angreppet är avsett att nå också andra personer är i stället förtalsbestämmelserna tillämpliga.

Ärekränkningsbrotten förtal och förolämpning kan också utgöra tryckfrihets- eller yttrandefrihetsbrott, dvs. ett yttrande som utgör

ett sådant brott kan vara straffbart trots att det görs i ett grundlagsskyddat medium. Angående denna fråga, se kapitel 23.

4.2.3 Brott mot tystnadsplikt

Den som röjer uppgift, som han är pliktig att hemlighålla enligt lag eller annan författning eller enligt förordnande eller förbehåll som har meddelats med stöd av lag eller annan författning, eller olovligen utnyttjar sådan hemlighet, döms enligt 20 kap. 3 § första stycket BrB för *brott mot tystnadsplikt* till böter eller fängelse i högst ett år. Om gärningen är belagd med straff enligt någon annan straffbestämmelse döms gärningsmannen dock enligt den bestämmelsen.

I 20 kap. 3 § andra stycket BrB föreskrivs att den som av oaktsamhet begår gärning som avses i första stycket, döms till böter. I ringa fall döms inte till ansvar.

Regleringen i 20 kap. 3 § BrB är den centrala straffrättsliga regleringen av överträdelser mot författningsreglerade tystnadsplikter. Röjandet av en uppgift kan ske i vilken form som helst, t.ex. muntligen, genom en skriftlig handling eller på ett elektroniskt medium.

Bestämmelser om tystnadsplikt som kan göra 20 kap. 3 § BrB tillämplig finns framför allt i sekretesslagen. Till den personkrets som omfattas av tystnadsplikt enligt sekretesslagen hör arbetstagare som är anställd hos myndigheten samt uppdragstagare, bland dem lekmannaledamöter i beslutande församlingar, i domstolar eller styrelser och nämnder inom förvaltningen. Totalförsvarspliktiga hör också till denna personkrets.

Också i andra författningar än sekretesslagen finns det föreskrifter om tystnadsplikt som omfattas av 20 kap. 3 § BrB. Som exempel kan nämnas tystnadsplikten för vissa tolkar och översättare, för personal inom enskilt bedriven hälso- och sjukvård, skolverksamhet och socialtjänst samt för advokater.

Om röjandet av en uppgift sker genom offentliggörande i tryckt skrift eller i något av de medier som omfattas av yttrandefrihetsgrundlagen eller genom meddelande för offentliggörande i något av dessa medier gäller tryckfrihetsförordningens och yttrandefrihetsgrundlagens regler till skydd för yttrandefriheten. Ansvar för en gärning som utgör brott mot tystnadsplikt kan då endast utdömas enligt dessa regler. Av de tryck- och yttrandefrihetsrättsliga

reglerna framgår att det alltid är straffbart att uppsåtligt åsidosätta en sekretessbestämmelse genom att den tystnadspliktige lämnar en hemlig handling för publicering eller på annat sätt, dock utan att ansvara för publiceringen, medverkar till att handlingen publiceras (7 kap. 3 § första stycket 2 TF och 5 kap. 3 § första stycket 2 YGL). Motsvarande gäller om den tystnadspliktige själv offentliggör den hemliga handlingen (7 kap. 5 § 1 TF och 5 kap. 1 § första stycket YGL). Det är också straffbart att i övrigt uppsåtligt åsidosätta en tystnadsplikt i de fall som anges i särskild lag. Den särskilda lag som här avses är sekretesslagen och närmare bestämt dess 16 kapitel. Där uppräknas de tystnadsplikter, s.k. kvalificerade tystnadsplikter, som har företräde framför rätten att fritt yttra sig (7 kap. 3 § första stycket 3 och 5 § 3 TF samt 5 kap. 1 § och 3 § första stycket 3 YGL).

Den som på angivet straffbart sätt lämnar hemlig handling för publicering eller på annat sätt, dock utan att ansvara för publiceringen, medverkar till att sådan handling publiceras döms för brott mot tystnadsplikt enligt 20 kap. 3 § BrB (7 kap. 3 § första stycket TF och 5 kap. 3 § första stycket YGL). Om den tystnadspliktige själv offentliggör den hemliga handlingen eller bryter sin kvalificerade tystnadsplikt döms denne för tryck- eller yttrandefrihetsbrott (7 kap. 5 § TF 5 kap. 1 § YGL).

4.3 Rätt till ersättning för kränkning

I skadeståndslagen (1972:207, SkadestL) finns grundläggande regler om i vilka sammanhang skada kan ge upphov till ersättning. Bestämmelserna i skadeståndslagen gäller om inte annat är särskilt föreskrivet eller föranleds av avtal eller i övrigt följer av regler om skadestånd i avtalsförhållanden (1 §).

I detta sammanhang är framför allt bestämmelsen i 2 kap. 3 § om rätt till ersättning för kränkning av intresse. Där föreskrivs att den som allvarligt kränker någon annan genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära skall ersätta den skada som kränkningen innebär.

Ersättning för kränkning är en särskild form av ideellt skadestånd som inte förutsätter att fysisk skada uppkommit (Bengtsson/Strömbäck, Skadeståndslagen, En kommentar, s. 58). Bestämmelsen i 2 kap. 3 § infördes år 2002 i samband med att ändringar gjordes i skadeståndslagen för att stärka rätten till

skadestånd för ideell skada (prop. 2000/01:68, bet. 2000/01:LU19) varigenom en tidigare regel om kränkningsersättning i 1 kap. 3 § upphävdes. Den nya bestämmelsen syftar till en förenklad och tydligare reglering. I regeringens proposition i ämnet anfördes bl.a. följande (s. 48):

> Utmärkande för de brott som grundar rätt till sådan ersättning som avses i 1 kap. 3 § är att de innefattar ett angrepp på den skadelidandes personliga integritet, här närmast dennes privatliv och människovärde. Kränkningsersättningen avser att kompensera känslor som den kränkande handlingen har framkallat hos den skadelidande, såsom rädsla, förnedring, skam eller liknande som inte tar sig sådana medicinska uttryck att det föreligger en personskada. Det ligger visserligen i sakens natur att själva kränkningen inte kan suddas ut genom ersättning i pengar. Ersättningen kan dock lindra verkningarna av kränkningen. Den kan bidra till att den skadelidande får upprättelse för den förnedrande och kränkande handlingen och därmed också bidra till att återställa självrespekten och självkänslan. Genom ersättningen kan den skadelidande t.ex. unna sig något extra och därigenom skingra tankarna på kränkningen och den olust och det obehag som han eller hon har åsamkats. Den som utsatts för mycket grova kränkningar kan få en möjlighet att genom ersättningen göra nödvändiga förändringar i sin livssituation. Detta torde vara vad som gäller enligt nuvarande bestämmelse, och enligt regeringens mening bör ersättningen även i fortsättningen inriktas på dessa fall.

Den generella rätten till kränkningsersättning enligt 2 kap. 3 § SkadestL förutsätter alltså en brottslig handling, detta till skillnad från vad som gäller på en rad särreglerade rättsområden. Inte heller enligt 2 kap. 3 § SkadestL krävs det emellertid att skadevållaren faktiskt fällts till ansvar för det aktuella brottet. Den skadelidande kan således ha rätt till ersättning även om det föreligger någon straffrihetsgrund eller om brottet är preskriberat.

När den nya regeln om rätt till kränkningsersättning infördes ville man som framgått inte upphäva sambandet mellan brott och skadestånd. Man framhöll att lagens krav på att den ersättningsgrundande handlingen skall vara brottslig knappast kunde slopas utan att det i stället uppställdes något annat allmänt kriterium som grund för ersättning. Kravet på brott hade enligt regeringen den fördelen att de fall där kränkningsersättning skall betalas avgränsas till handlingar som av lagstiftaren definierats som klandervärda. För att ett brott skall föreligga skall dels den begångna handlingen var otillåten, dels gärningsmannen ha ett personligt ansvar. Man framhöll vidare att praxis utvisat att

kränkningsersättning även kan utgå i vissa särskilda fall vid brott som inte är uppsåtliga. Detta borde också gälla enligt den nya bestämmelsen.

Med kränkning genom brott som innefattar ett angrepp mot *annans person* avses ett angrepp mot den kroppsliga integriteten. Hit hör bl.a. sexualbrott, misshandel, grov misshandel och försök till mord samt våld mot tjänsteman, förgripelse mot tjänsteman och övergrepp i rättssak.

Angrepp mot annans frihet syftar på den enskildes rörelse- och handlingsfrihet. Exempel på sådana brott är människorov, olaga frihetsberövande, försättande i nödläge och olaga tvång.

Med *angrepp mot annans frid* avses främst brott som kränker den enskildes rätt att få vara ifred och att hålla sitt privatliv okänt för andra. Hit hör brotten olaga hot och de tidigare beskrivna brotten hemfridsbrott, ofredande, brytande av post- och telehemlighet, intrång i förvar och olovlig avlyssning. Andra exempel är hot mot tjänsteman samt – om gärningen innefattar hot – förgripelse mot tjänsteman och övergrepp i rättssak. Till denna brottskategori hör också överträdelse av besöksförbud som är ägnad att oroa den skyddade samt vissa förmögenhetsbrott med särskilt hänsynslösa och kränkande inslag, t.ex. grov stöld i en bostad som vandaliserats.

Angrepp mot annans ära tar sikte på kränkningar av någon annans anseende eller självkänsla. I första hand avses ärekränkningsbrotten. Hit hör också mened, om gärningsmannen haft uppsåt att skada en oskyldig person. Detsamma gäller falskt eller obefogat åtal, falsk eller obefogad angivelse samt falsk eller vårdslös tillvitelse.

Den som orsakat en allvarlig kränkning genom sådant brott som sägs i 2 kap. 3 § SkadestL skall ersätta den skada som kränkningen innebär. Begreppet skada är här avsett att väsentligen motsvara det begrepp – lidande – som även tidigare använts för motsvarande situationer, dock med den skillnaden att det i mindre mån syftar på den skadelidandes egen upplevelse. Avsikten är alltså att skadan i huvudsak skall bedömas utifrån objektiva kriterier. Sådana kriterier anges i 5 kap. 6 § SkadestL, där det finns riktlinjer för hur ersättningen skall bestämmas. Av motiven till den bestämmelsen framgår att det emellertid också bör finnas ett visst utrymme att ta hänsyn till den drabbades upplevelse i det enskilda fallet.

4.4 Visst skydd som gäller mellan enskilda m.m.

4.4.1 Rätten till namn och bild i reklam

År 1979 infördes, på grundval av förslag från 1966 års integritetsskyddskommitté, lagen (1978:800) om namn och bild i reklam. Vid lagens tillkomst anförde föredragande statsrådet bl.a. följande (prop. 1978/79:2 s. 3 f.):

> Även om det inte alltid behöver vara förenat med obehag för den enskilde att förekomma i reklam, kan det naturligtvis vara det. Det framstår närmast som en självklarhet att den enskilde själv måste få bestämma om han över huvud taget vill bli utnyttjad för reklamändamål och vad han i så fall vill göra reklam för. Med den omfattning och genomslagskraft som den moderna marknadsföringen har är det av central betydelse för den enskilde att kunna förhindra att hans bild eller namn förknippas med produkter eller tjänster som han inte gillar.

Enligt 1 § får näringsidkare vid marknadsföring av vara, tjänst eller annan nyttighet inte använda framställning i vilken annans namn eller bild utnyttjas utan dennes samtycke. Med namn jämställs annan beteckning som klart utpekar viss person.

Vad som sägs om näringsidkare i bestämmelsen gäller även anställd.

Skyddet mot bildanvändning avser inte bara s.k. kändisar, utan varje bildanvändning av en identifierbar person omfattas. Detta gäller alltså även om denne person skulle vara okänd för allmänheten (KARNOV 2006/07, s. 1746).

Den som uppsåtligen eller av grov oaktsamhet gör sig skyldig till sådant olovligt utnyttjande av namn eller bild som avses i 1 § skall enligt 2 § dömas till böter.

I 3 § första stycket anges att den som bryter mot 1 § eller medverkar till sådan handling som där sägs skall utge skäligt vederlag till den vars namn eller bild har utnyttjats. Sker det uppsåtligen eller av oaktsamhet, skall ersättning utgå också för annan skada. Vid bedömningen av i vad mån sådan skada har uppstått tas hänsyn även till lidande och andra omständigheter av annan än rent ekonomisk betydelse.

Av andra stycket i samma paragraf följer bl.a. att en arbetsgivare är skyldig att utge vederlag för ersättningsgrundande handling som någon anställd utfört i hans tjänst.

Bestämmelsen om vederlag innebär att oavsett om förutsättningar för straff föreligger (för vilket krävs uppsåt eller

grov oaktsamhet) har den som utsätts för ett personlighetsintrång enligt denna lag alltid rätt till ersättning för utnyttjandet (KARNOV 2006/07, a. st.).

Lagen är tillämplig bara på kommersiell reklam, dvs. reklam som avser varor och tjänster eller som på något annat sätt har till syfte att öka omsättningen för en näringsidkare. Så kallad ideell reklam, t.ex. information eller propaganda från politiska partier eller från religiösa eller andra ideella sammanslutningar, berörs således inte av lagen. Som skäl för detta anfördes i förarbetena bl.a. att en straffrättslig reglering av missbruk av namn och bild i ideell reklam skulle få konsekvenser i tryckfrihetsrättsligt hänseende, eftersom endast den kommersiella reklamen men inte den ideella reklamen anses falla utanför delar av den tryckfrihetsrättsliga regleringen (a. prop. s. 59 f.)

4.4.2 Namnlagen

Lagregler om namnskydd är i vårt land av ganska sent datum. Ett mer allmänt system av regler i syfte att förhindra de tidigare i stor omfattning förekommande fria namnbytena kom till i början av 1900-talet. Regler om familjerättsliga namnförvärv infördes därefter under perioden 1915–1920 genom giftermålsbalken och andra familjerättsliga lagar. Reglerna samlades i en och samma lag genom 1963 års namnlag. Denna lag har därefter ersatts av 1982 års namnlag, som alltjämt gäller (SFS 1982:670).

Lagens 1–10 §§ innehåller bestämmelser om familjerättsliga förvärv av namn.

En utgångspunkt i 1982 års lag är att den enskilde i så stor utsträckning som möjligt skall få bestämma vilket namn han eller hon skall ha (prop. 1981/82:156 s. 14 f.). Strävanden efter jämställdhet mellan könen har också haft ett stort inflytande på de nya reglerna. En konsekvens blev att ett efternamn i större utsträckning än tidigare kunde komma att ledas utanför den ursprungliga släktkretsen och att det släktnamnsbegrepp som använts i 1963 års namnlag ersattes med det mera neutrala begreppet efternamn.

I 13 § finns bestämmelser om skydd för namn och andra kännetecken som tillkommer någon annan. Där sägs i första stycket att som efternamn, vare sig det är nybildat eller inte, får inte godkännas namn som lätt kan förväxlas med

1. ett efternamn som någon annan enligt lag bär eller har rätt att bära,
2. ett allmänt känt efternamn som har burits av en utdöd släkt,
3. ett allmänt känt utländskt efternamn,
4. någon annans konstnärsnamn eller ett likartat namn som är allmänt känt,
5. en beteckning för en stiftelse, en ideell förening eller någon annan liknande sammanslutning,
6. någon annans här i riket skyddade firma eller varumärke eller ett annat kännetecken som har inarbetats för någon annan i en näringsverksamhet här i riket, eller
7. en titel på någon annans skyddade litterära eller konstnärliga verk, om titeln är egenartad, eller ett särskilt skapat namn som förekommer i ett sådant verk och vars utnyttjande skulle innebära en kränkning av någon annans upphovsrätt till verket.

I 13 § andra stycket finns bestämmelser om s.k. anslutningsförvärv, dvs. om föräldrars, syskons eller syskonbarns möjligheter att erhålla ett nybildat efternamn.

Vidare föreskrivs i 17 § att om någon efter ansökan hos Patent- och registreringsverket har bytt till ett efternamn som han eller hon inte har burit tidigare och det uppstår olägenhet för någon annan till följd av sådan risk för förväxling som anges i 12 § första stycket, skall domstol på talan av den andre besluta att den som har erhållit namnet förlorar detta, om inte synnerliga skäl talar för att han eller hon får behålla det. Den som på detta sätt förlorar sitt namn återfår det efternamn han eller hon hade före ansökningen.

I namnlagen finns också ett särskilt skydd för egenartade efternamn. Således föreskrivs i 20 § första stycket att om någon har förvärvat ett egenartat efternamn, får ett namn som lätt kan förväxlas med detta användas av någon annan endast om han eller hon enligt namnlagen kan åberopa rätt till namnet eller om han eller hon eller släkten av ålder eller annars enligt ortens sed har burit det som tillnamn. I paragrafens andra stycke sägs att ingen obehörigen får, till nackdel för den som har förvärvat ett egenartat efternamn, i näringsverksamhet använda en firma, ett varumärke eller ett annat kännetecken som lätt kan förväxlas med namnet. I ett tredje stycke föreskrivs att efternamn skall anses som egenartat om det är ägnat att utmärka tillhörigheten till en viss släkt.

Den som gör intrång i någon annans rätt till ett egenartat efternamn är enligt 23 § skyldig att ersätta den andres skada, om

han eller hon har insett eller borde ha insett att förfarandet var till nackdel för denne. Vid bedömande om och i vad mån skada har uppstått skall hänsyn tas även till lidande och omständigheter av annan än rent ekonomisk betydelse.

4.4.3 Sekretesskydd för fotografier i offentliga register

Den 1 juli 2004 infördes i 7 kap. 15 § andra stycket SekrL en förstärkt sekretess för fotografier i offentliga register. Rikspolisstyrelsens centrala passregister och Vägverkets vägtrafikregister utgör exempel på register som innehåller fotografier av enskilda. Sekretessen gäller om det inte står klart att uppgiften kan lämnas ut utan att den enskilde eller någon närstående till denne lider men, dvs. med presumtion för sekretess.

Beträffande avvägningen mellan insynsintresset och den enskildes intresse av skydd anförde regeringen att mediernas tillgång till fotografier av personer som i skilda egenskaper utövar makt i samhället eller annars spelar en roll i skildringen eller granskningen av samhälleliga missförhållanden var, med hänsyn till handlingsoffentlighetens allmänna syften, av särskilt stor betydelse (prop. 2003/04:93 s. 37 f.). Häremot skulle ställas det obehag och den rädsla enskilda känner när fotografier som föreställer dem själva, och som de har lämnat in till en myndighet för att t.ex. få körkort, senare används vid gärningar som kanske utgör hotbrott eller förekommer i sammanhang som annars upplevs som hotfulla. Enligt regeringen gick det inte heller att bortse från att det finns en risk för att t.ex. offentliga tjänstemän, som blir föremål för registrering av personer om vilka det är känt att de inte är främmande för att begå våldshandlingar eller som får sin bild publicerad i ett sammanhang som utgör olaga hot eller annars upplevs som hotfullt, av rädsla för trakasserier eller våldshandlingar avstår från berättigade ingripanden eller andra åtgärder. Det borde också beaktas att en förstärkt sekretess för fotografier i de offentliga registren inte leder till att sådana allmänna handlingar i myndigheternas förvar som innehåller sakuppgifter eller bedömningar blir mer svåråtkomliga. Enligt regeringen skulle således mediernas möjlighet att i sak fullfölja sitt angelägna samhällskritiska uppdrag inte begränsas, även om en förstärkt sekretess skulle medföra att t.ex. dagspressen ofta skulle vägras tillgång till fotografier ur de offentliga registren.

Ett omvänt skaderekvisit bör leda till att varje begäran att få ta del av ett fotografi bedöms ingående. Den som begär att få ta del av fotografier får redogöra dels för sin identitet, dels för syftet med sin begäran. Att regelmässigt göra anonyma uttag brevledes, per fax eller e-post är vid en tillämpning av detta rekvisit inte möjligt (Regner m.fl., Sekretesslagen, En kommentar, s. 7:79). När ett fotografi är avsett att publiceras i ett sammanhang som är negativt för den enskilde eller – i de fall den som fotografiet föreställer är avliden – publiceringen sker på ett sätt eller i ett sammanhang som kan uppfattas som negativt av de närstående, kommer utgångspunkten vara att fotografiet omfattas av sekretess. Det gäller även om den tilltänkta publiceringen motiveras av ett starkt allmänintresse (a. prop. s. 40).

4.5 Skydd vid behandling av personuppgifter

Användningen av datorer har alltsedan de första datamaskinerna började användas ansetts medföra särskilda problem från integritetssynpunkt på grund av de möjligheter som datortekniken innebär i fråga om att sammanställa, lagra och sprida stora mängder av information om enskilda personer. Denna teknik kom därför tidigt att kringgärdas av en särskild skyddsreglering. Det dröjde emellertid till 1989 innan det i grundlagen – i 2 kap. 3 § andra stycket RF – infördes en bestämmelse om att en sådan skyddsreglering skall finnas.

Den svenska lagstiftningsmodellen har varit att använda sig av en generellt tillämplig reglering, dvs. en som gäller både för myndigheter och för enskilda. Så var fallet med den tidigare datalagen (1973:289) och så är också den nu gällande personuppgiftslagen (1998:204) utformad. Uteslutande privat behandling av personuppgifter har traditionellt varit oreglerad. Vidare har man tillämpat den ordningen att i den mån särskilda regler utfärdats, har dessa gällt framför den generella regleringen. På myndighetsområdet har det därför under lång tid varit möjligt att upprätthålla ett system med särregler i s.k. registerförfattningar. För särskilt viktiga register eller för register som innehåller en stor mängd känsliga personuppgifter har sådana författningar utfärdats i form av lag.

Riskerna för integriteten i samband med användningen av datorteknik har också ansetts kräva en särskild sekretessregel vid

utlämnande av personuppgifter från en myndighet genom en allmän handling eller på annat sätt. I 7 kap. 16 § SekrL anges sålunda att sekretess gäller för personuppgift, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Denna bestämmelse har i den allmänna debatten kritiserats för att i alltför hög grad tillgodose integritetsskyddsintresset på bekostnad av offentlighetsintresset. Tidigare fanns en bestämmelse i datalagen med motsvarande innehåll som gällde för enskilda vid deras utlämnande av personuppgifter. Regler för enskilda finns numera i personuppgiftslagen, i första hand i 9 och 10 §§.

I kommitténs direktiv framhålls att det på IT-området redan finns en omfattande lagstiftning till skydd för den personliga integriteten. Enligt direktiven kan det dock med hänsyn till den snabba utvecklingen finnas anledning att översiktligt granska om den befintliga lagstiftningen ger ett tillfredsställande skydd på IT-området.

Nedan redogörs för sådan gällande rätt som rör skyddet för personuppgifter vid framför allt behandling med hjälp av datorteknik. Härvid beskrivs kortfattat det EG-direktiv som ligger till grund för den svenska skyddslagstiftningen på området. Vidare omnämns vissa internationella regler på dataskyddsområdet. Något mer utförligt redogörs för den lag genom vilken EG-direktivet införlivats i svensk lagstiftning, dvs. personuppgiftslagen. I sammanhanget redovisas också den reform som nyligen genomförts i syfte att åstadkomma en viss avreglering och avkriminalisering på området. Avslutningsvis redovisas den nyss angivna särskilda sekretessbestämmelsen – 7 kap. 16 § SekrL – som syftar till att skydda personuppgifter vid framför allt automatiserad databehandling.

De registerförfattningar som finns på olika verksamhetsområden redovisas inte här utan först i samband med respektive verksamhetsområde. Särskilt skydd för personuppgifter finns därutöver på området för elektroniska kommunikationstjänster och vid allmän kameraövervakning. Dessa regler redovisas inte heller här, utan i samband med redogörelsen för respektive område (se nedan kapitel 15 och 16).

4.5.1 Vissa internationella regler och riktlinjer

Förenta nationerna

Förenta nationernas (FN) generalförsamling antog år 1990 riktlinjer om datoriserade register med personuppgifter. Riktlinjerna återges i sin helhet i betänkandet *Översyn av personuppgiftslagen* (SOU 2004:6), s. 44 f.

Europarådet

Även inom Europarådet har antagits regler som särskilt rör automatiserad behandling av personuppgifter. År 1980 antogs en konvention (nr 108) till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen. Samtliga EU- och EES-stater har ratificerat konventionen. Till konventionen har också utarbetats ett tilläggsprotokoll om tillsynsmyndigheter och flödet av personuppgifter över gränserna samt en rad rekommendationer. Dataskyddskonventionens syfte är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatisk databehandling av personuppgifter. Utgångspunkten är att vissa av den enskildes rättigheter kan behöva skyddas i förhållande till den princip om fritt flöde av information, oberoende av gränser, som finns inskriven i internationella överenskommelser om mänskliga rättigheter. Inget hindrar att registrerade personer tillerkänns ett mer omfattande skydd än som föreskrivs i konventionen.

OECD

En expertgrupp inom Organisationen för ekonomiskt samarbete och utveckling (OECD) har utarbetat vissa riktlinjer som rör integritetsskydd och flödet av personuppgifter över gränserna. Riktlinjerna antogs år 1980 av OECD:s råd tillsammans med en rekommendation till medlemsländernas regeringar att beakta riktlinjerna i nationell lagstiftning. Samtliga medlemsländer, dvs. även Sverige, har godtagit rekommendationen och därmed åtagit sig att följa denna. Riktlinjerna är tillämpliga på personuppgifter inom både den offentliga och den privata sektorn.

4.5.2 EG:s dataskyddsdirektiv

År 1995 antogs Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (härefter dataskyddsdirektivet).

Enligt artikel 1 punkt 1 skall medlemsstaterna i enlighet med detta direktiv skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter.

Vidare sägs att medlemsstaterna varken får begränsa eller förbjuda det fria flödet av personuppgifter mellan medlemsstaterna av skäl som har samband med det under punkt 1 föreskrivna skyddet.

Syftet med dataskyddsdirektivet är således att skapa en gemensam, hög nivå på integritetsskyddet för att därigenom möjliggöra ett fritt flöde av personuppgifter medlemsländerna emellan. En bakomliggande tanke är också att en harmoniserad lagstiftning på detta område är ägnad att undanröja hinder för den inre marknadens förverkligande. Medlemsstaterna får inom den ram som ges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Dessa preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen.

I artikel 3 anges direktivets tillämpningsområde. Direktivet är tillämpligt på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg liksom på manuell behandling av personuppgifter som ingår i eller kommer att ingå i ett register (av artikel 2 framgår att med register avses varje strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier).

Vidare sägs att direktivet inte gäller för sådan behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten (exempelvis allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område). Det är inte heller tillämpligt på sådan behandling av personuppgift som utförs av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll.

Dataskyddsdirektivet har införlivats med svensk lagstiftning genom personuppgiftslagen (1998:204). Personuppgiftslagen följer i huvudsak direktivets text och disposition. Någon ytterligare

redovisning av själva direktivets innehåll lämnas därför inte här. Dataskyddsdirektivet finns återgivet i sin helhet i bl.a. SOU 2004:6.

4.5.3 Personuppgiftslagen

Tillämpningsområde

Som nämnts ovan har dataskyddsdirektivet införlivats med svensk lagstiftning genom personuppgiftslagen (1998:204). Lagen gäller för sådan behandling som är helt eller delvis automatiserad (5 §). Den gäller också för annan behandling av personuppgifter om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen trädde i kraft den 24 oktober 1998. I fråga om automatiserad behandling fick den på grund av övergångsbestämmelser fullt genomslag först den 1 oktober 2001. Beträffande annan behandling av personuppgifter gäller lagen inte fullt ut förrän den 1 oktober 2007.

Till skillnad från dataskyddsdirektivet är personuppgiftslagen inte begränsad till verksamhet som omfattas av EG-rätten, utan den är generellt tillämplig på sådan behandling som lagen tar sikte på. Lagen är subsidiär i förhållande till annan lag eller förordning (2 §). Vid dess införande anfördes att det traditionella svenska systemet med särregler i särskilda författningar var att föredra framför generella undantag från den nya lagen (prop. 1997/98:44 s. 41). I detta sammanhang framhölls också att det inte fanns anledning att avvika från det tidigare uttalade målet att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll skall regleras särskilt i lag (se prop. 1990/91:60 s. 50 och bet. 1990/91:KU 11 s. 11).

Ett arbete med att se över gällande registerförfattningar inleddes med anledning av att personuppgiftslagen infördes. Detta arbete pågår alltjämt.

Inledningsvis bör också nämnas att ändringar i personuppgiftslagen trädde i kraft den 1 januari 2007 som syftade till att underlätta behandling av personuppgifter i löpande text och annat ostrukturerat material. Vid sådan behandling gäller inte längre flertalet av hanteringsreglerna i lagen. En viss avkriminalisering infördes också som innebär att gärningar som begås av

oaktsamhet inte längre är straffbara. Den redovisning som lämnas nedan tar sikte på huvudreglerna i lagen. Avslutningsvis lämnas en närmare redogörelse för den nu nämnda avregleringen av behandling i löpande text och för avkriminaliseringen.

Undantag från personuppgiftslagen

Enligt 6 § gäller lagen inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur.

Vidare föreskrivs i 7 § första stycket att bestämmelserna i lagen inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Av 7 § andra stycket framgår att huvuddelen av lagens bestämmelser inte heller skall tillämpas på sådan behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Bestämmelserna i 30–32 §§ om säkerhetsåtgärder skall dock tillämpas.

Beträffande 7 § konstaterades vid lagens införande att dataskyddsdirektivet tillåter att nödvändiga undantag görs för all behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande (prop. 1997/98:44 s. 52). Det framhölls att all journalistisk, konstnärlig eller litterär verksamhet inte har grundlagsskydd, eftersom grundlagsskyddet för tryckfriheten och yttrandefriheten inte avser alla former av yttranden. Emellertid ansågs att de nämnda slagen av verksamhet har så stor betydelse att de måste kunna bedrivas obehindrat. Det undantag från den nya lagens hanteringsbestämmelser som dataskyddsdirektivet medger borde därför utnyttjas fullt ut.

Frågan om vad som utgör behandling av personuppgifter uteslutande för journalistiskt ändamål i enlighet med 7 § andra stycket har prövats av Högsta domstolen i det s.k. *Ramsbro-målet* (NJA 2001 s. 409). I det målet hade en man under namnet Stiftelsen mot Nordbanken inrättat en webbplats på Internet. Åtalet gällde att han där lagt ut såväl kränkande som andra personuppgifter varigenom uppgifterna förts över till tredje land. Högsta domstolen anförde bl.a. att det fick anses vara uppenbart att tolkningen av artikel 9 i dataskyddsdirektivet (som ligger till grund för 7 § andra stycket PuL) skall ske med särskilt beaktande

av Europakonventionen. Man påpekade att Europakonventionen gäller som svensk lag här i landet sedan den 1 januari 1995 och att lag eller annan föreskrift inte får meddelas i strid med konventionen enligt 2 kap. 23 § regeringsformen. Vidare konstaterade man att rättigheterna enligt artikel 8 (skydd för privatlivet) och artikel 10 (yttrandefrihet) i Europakonventionen kan i enskilda fall komma i konflikt med varandra samt att Europadomstolen vid sådana konflikter tillämpar den s.k. proportionalitetsprincipen, vilket innebär att en avvägning görs mellan intresset av skydd för privatlivet och intresset av yttrandefrihet. Domstolen anförde att det får antas att det i personuppgiftslagen beskrivna, på direktivet grundade, undantaget för journalistiska ändamål utgör ett försök att i mer generella termer ge uttryck för en sådan intresseavvägning. Att uttrycket journalistiska ändamål använts kunde under sådana förhållanden inte antas vara i avsikt att privilegiera etablerade massmedier eller personer som är yrkesverksamma inom sådana medier. Med uttrycket torde snarare få anses vara avsett att betona vikten av en fri informationsspridning i frågor av betydelse för allmänheten eller för grupper av människor och en fri debatt i samhällsfrågor.

Sammanfattningsvis fann Högsta domstolen att det inte var visat annat i målet än att mannens behandling av personuppgifter på den aktuella webbsidan skett uteslutande för journalistiska ändamål. Han skulle därför inte dömas till ansvar för den åtalade gärningen.

Enligt 8 § första stycket skall bestämmelserna i lagen inte tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. TF att lämna ut personuppgifter, dvs. inom ramen för principen om allmänna handlingars offentlighet. Lagrummet kan jämföras med punkt 72 i ingressen till det bakomliggande EG-direktivet: ”Detta direktiv gör det möjligt att vid genomförandet av dessa bestämmelser ta hänsyn till principen om allmänna handlingars offentlighet”.

Vidare föreskrivs i 8 § andra stycket att bestämmelserna i lagen inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Av förarbetena framgår att det inte förutsätts att bevarandet är föreskrivet i författning (prop. 1997/98:44 s. 119 f.). Det är tillräckligt att det är fråga om allmänna handlingar.

Grundläggande krav

Personuppgiftslagen innehåller vissa grundläggande krav på behandlingen av personuppgifter (9 §). Den personuppgiftsansvarige, vilken oftast är den organisation där personuppgifterna behandlas, skall se till att personuppgifter behandlas bara om det är lagligt och att de alltid behandlas på ett korrekt sätt och i enlighet med god sed.

Vidare skall personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. De får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Det sistnämnda kan bli aktuellt att pröva när personuppgifter lämnas ut till tredje man. Ett sådant utlämnande får alltså inte vara oförenligt med det ändamål för vilket uppgifterna ursprungligen samlades in. Om personuppgifter lämnas ut i form av allmänna handlingar med stöd av bestämmelserna i 2 kap. TF blir en sådan prövning dock inte aktuell.

De personuppgifter som behandlas skall vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Inte heller får fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Därutöver skall de uppgifter som behandlas vara riktiga och, om det är nödvändigt, aktuella. Alla rimliga åtgärder skall vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

För behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål gäller vissa särregler.

När behandling är tillåten

I 10 § anges vilka krav som i allmänhet måste vara uppfyllda för att behandling av personuppgifter skall vara tillåten.

Som huvudregel gäller att behandling av personuppgifter är tillåten bara om den registrerade har lämnat sitt samtycke till behandlingen. Har så inte skett får behandling ändå ske om den är nödvändig för att

a) ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,
b) den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet,
c) vitala intressen för den registrerade skall kunna skyddas,
d) en arbetsuppgift av allmänt intresse skall kunna utföras,
e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller
f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifter lämnas ut skall kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot den personliga integriteten.

Vid lagens införande konstaterades att behandling av personuppgifter som rör direkt marknadsföring kan vara tillåten med stöd av en sådan intresseavvägning som anvisas i punkt f (prop. 1997/98:44 s. 66), trots att den registrerade inte har lämnat sitt samtycke till behandlingen. Om den registrerade skriftligen har anmält att han eller hon motsätter sig sådan behandling innehåller lagen ett uttryckligt förbud mot behandling av personuppgifter för sådana ändamål (11 §).

Numera finns centrala och allmänt tillgängliga register dit enskilda kan anmäla att de inte vill ha direktadresserad reklam eller reklamerbjudanden per telefon. I detta sammanhang kan också nämnas att det enligt marknadsföringslagen (1995:450), om samtycke inte föreligger, som huvudregel är förbjudet med marknadsföring genom e-post, telefax eller sådana uppringningsautomater eller andra liknande automatiska system för individuell kommunikation som inte betjänas av någon enskild.

Känsliga personuppgifter

Enligt 14 § är det generellt sett förbjudet att behandla känsliga personuppgifter. Med känsliga uppgifter avses ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening eller uppgifter som rör hälsa eller sexualliv.

Från förbudet att behandla känsliga personuppgifter finns vissa undantag. Sålunda är det tillåtet att behandla känsliga personuppgifter, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort uppgifterna (15 §).

Även om uttryckligt samtycke inte föreligger får enligt 16 § personuppgifter behandlas om behandlingen är nödvändig för att

a) den personuppgiftsansvarige skall kunna fullgöra sina skyldigheter inom arbetsrätten,
b) den registrerades eller någon annans vitala intressen skall kunna skyddas och den registrerade inte kan lämna sitt samtycke, eller
c) rättsliga anspråk skall kunna fastställas, göras gällande eller försvaras.

Undantag från kravet på uttryckligt samtycke gäller även vid behandling inom ideella organisationer (17 §) och inom hälso- och sjukvården (18 §).

Vidare finns ett undantag som gäller behandling av känsliga personuppgifter inom området för forskning och för statistikändamål (19 §). I det förstnämnda fallet är behandling tillåten om den godkänts enligt lagen (2003:460) om etikprövning av forskning som avser människor. I det sistnämnda fallet kan behandlingen vara tillåten om samhällsintresset av statistikprojektet klart väger över riskerna för otillbörligt intrång i den personliga integriteten. Denna förutsättning skall anses vara uppfylld om en forskningsetisk kommitté har godkänt behandlingen.

Enligt 20 § får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om ytterligare undantag från förbudet att behandla känsliga personuppgifter, om det behövs med hänsyn till ett viktigt allmänt intresse.

Uppgifter om lagöverträdelser

En annan kategori av personuppgifter som har reglerats särskilt är uppgifter om lagöverträdelser. I 21 § sägs att det är förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Dock har regeringen eller den myndighet som regeringen bestämmer bemyndigats att meddela undantag från detta förbud. Vidare får

regeringen i enskilda fall besluta om undantag. Regeringen får också överlåta åt tillsynsmyndighet att fatta sådana beslut.

Behandling av personnummer

Enligt artikel 8.7 i dataskyddsdirektivet skall medlemsstaterna bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Direktivet innebär alltså att det i Sverige måste finnas en reglering för användningen av personnummer. Däremot innehåller direktivet inte några bestämmelser om hur denna reglering skall se ut.

Vid personuppgiftslagens införande valde man att i princip oförändrade föra över reglerna om användning av personnummer i den dåvarande datalagen (1973:289) till den nya lagen (prop. 1997/98:44 s. 76 f.). Därmed gäller fortfarande att personnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller något annat beaktansvärt skäl (22 §). Denna bestämmelse i personuppgiftslagen gäller numera också sådant samordningsnummer som i stället för personnummer tilldelas personer som fr.o.m. den 1 januari 2000 inte är eller har varit folkbokförda här i landet (prop. 1999/2000:6, bet. 1999/2000:SkU7).

Information till den registrerade

Personuppgiftslagen skiljer på två olika slag av information till den registrerade; information som skall lämnas självmant av den personuppgiftsansvarige och information som skall lämnas efter ansökan.

Om uppgifter om en person samlas in från personen själv skall enligt 23 § den personuppgiftsansvarige i samband därmed självmant lämna information om den behandling man avser att företa.

Även om uppgifter har samlats in från någon annan än den registrerade skall den personuppgiftsansvarige självmant lämna information (24 §). I detta fall behöver informationen dock lämnas först när uppgifterna registreras. Om uppgifterna är avsedda att lämnas till tredje man, behöver information inte ges förrän uppgifterna lämnas ut för första gången.

Det finns dock undantag från skyldigheten enligt 24 § att självmant lämna information. Information behöver inte lämnas om det finns bestämmelser om registrerandet eller utlämnandet i lag eller annan författning. Inte heller behöver information lämnas, om det visar sig omöjligt – ett undantag som förefaller ganska självklart – eller skulle innebära en oproportionerligt stor arbetsinsats. Om uppgifterna används för att vidta åtgärder som rör den registrerade, skall emellertid information lämnas senast i samband med att så sker.

Den information som lämnas enligt 23 och 24 §§ skall omfatta uppgift om den personuppgiftsansvariges identitet, ändamålet med behandlingen och all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter i samband med behandlingen (25 §). Som exempel på sådan information nämns mottagarna av uppgifterna, samt skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse. Information behöver dock inte lämnas om sådant som den registrerade redan känner till.

De fall då den personuppgiftsansvarige är skyldig att lämna information efter ansökan tas upp i 26 §. En gång per kalenderår skall till var och en som ansöker om det lämnas besked huruvida personuppgifter som rör den sökande behandlas eller ej. Sådant besked skall vara gratis. Om uppgifter behandlas skall den personuppgiftsansvarige skriftligen lämna information om vilka uppgifter som behandlas, varifrån uppgifterna har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

Rättelse

Enligt 28 § är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller i enlighet med föreskrifter som har meddelats med stöd av lagen.

Om den registrerade begär det skall den personuppgiftsansvarige också underrätta den tredje man som uppgifterna har lämnats till om rättelseåtgärden. Även om den registrerade inte har begärt det är den personuppgiftsansvarige skyldig att underrätta tredje man angående en rättelseåtgärd, om mera betydande skada eller olägen-

het därmed kan undvikas för den registrerade. Någon skyldighet att underrätta tredje man föreligger dock inte om det skulle visa sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Automatiserade beslut

I personuppgiftslagen finns i 29 § en bestämmelse som reglerar vad som gäller i fråga om s.k. automatiserade beslut. Bestämmelsen avser beslut som grundas enbart på sådan automatiserad behandling av personuppgifter som är avsedda att bedöma egenskaper hos den berörda personen. Med egenskaper avses här personliga egenskaper såsom arbetsprestationer, kreditvärdighet, pålitlighet och uppträdande (prop. 1997/98:44 s. 88). Om ett sådant beslut har rättsliga följder för en fysisk person eller annars har märkbara verkningar för denne, skall den som berörs av beslutet ha möjlighet att på begäran få beslutet omprövat. Rätten av få ett automatiserat beslut omprövat innebär en rätt att få beslutet granskat av en person som har makt att ersätta det automatiserade beslutet med ett annat (prop. 1997/98:44 s. 135).

Var och en som har varit föremål för ett sådant automatiserat beslut som nu avses har också rätt att på ansökan få information från den personuppgiftsansvarige om vad som har styrt den automatiserade behandling som har lett fram till beslutet.

Överföring av personuppgifter till tredje land

Enligt 33 § personuppgiftslagen är det som huvudregel förbjudet att till tredje land (dvs. ett land som varken ingår i EU eller är anslutet till EES-samarbetet) föra över personuppgifter som är under behandling, om landet inte har en adekvat nivå för skyddet av personuppgifter. Detsamma gäller vid överföring av personuppgifter för behandling i tredje land. Förbudet gäller i princip alla slag av personuppgifter och är alltså inte begränsat till exempelvis kategorierna känsliga uppgifter eller uppgifter om lagöverträdelser. Även en sådan till synes harmlös uppgift som att en viss person har skadat en fot omfattas av förbudet (se EG-domstolens dom i målet Bodil Lindqvist, C-101/01, det s.k. konfirmandlärarmålet varom mera nedan).

Frågan om en adekvat skyddsnivå föreligger skall bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt skall läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen skall pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet.

Paragrafen fick sin nuvarande lydelse den 1 januari 2000. Den tidigare lydelsen ansågs innebära ett mer strikt överföringsförbud, som också träffade uppgifter som inte alls var känsliga från integritetssynpunkt och som knappast behövde något särskilt skydd. Redan vid den tidpunkt då personuppgiftslagen skulle träda i kraft möttes reglerna om överföring av uppgifter till tredje land av kritik. Reglerna ansågs medföra en oönskad begränsning av möjligheten att använda sig av modern informationsteknik, som t.ex. elektronisk post och elektroniska anslagstavlor (se t.ex. bet. 1998/99:KU15). I debatten nämndes exempel där en tillämpning av reglerna ansågs leda till orimliga resultat, eftersom uppgifterna bedömdes vara harmlösa i den mening att en spridning av uppgifterna inte borde leda till någon integritetskränkning.

Regeringen föreslog därför i oktober 1999 att bestämmelsen om överföring av personuppgifter till tredje land skulle få den lydelse som den nu har (prop. 1999/2000:11). Riksdagen antog regeringens förslag (bet. 1999/2000:KU7). Därmed kom lydelsen att närmare ansluta till motsvarande bestämmelse i EG-direktivet. Överföring till tredje land kom härigenom inte längre att vara förbjuden om skyddsnivån i det tredje landet är adekvat. Vidare fördes i den svenska lagtexten in de omständigheter som enligt EG-direktivet skall tilläggas särskild vikt vid prövningen om ett tredje lands skyddsnivå är adekvat. Det bör emellertid observeras att det även enligt den nya lydelsen är i princip förbjudet att föra över personuppgifter till ett land där skyddsnivån inte är adekvat.

Från förbudet enligt 33 § finns vissa generella undantag i 34 §. Dessa innebär att en överföring av personuppgifter till tredje land i vissa situationer är tillåten även om landet eller länderna i fråga inte har en adekvat skyddsnivå. Sådana undantagsfall föreligger om överföringen är nödvändig för att

a) ett avtal mellan den registrerade och den personuppgifts-ansvarige skall kunna fullgöras eller åtgärder som registrerade begärt skall kunna vidtas innan ett avtal träffas,

b) ett sådant avtal mellan den personuppgiftsansvarige och tredje man som är i den registrerades intresse skall kunna ingås eller fullgöras,
c) rättsliga anspråk skall kunna fastställas, göras gällande eller försvaras, eller
d) vitala intressen för den registrerade skall kunna skyddas.

Det är enligt samma paragraf också tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.

I 35 § finns vissa bemyndiganden som avser möjligheten att besluta om ytterligare undantag från förbudet i 33 §. Regeringen får meddela föreskrifter om sådant undantag för överföring till vissa stater eller för det fall att överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter. Under dessa förutsättningar kan regeringen också besluta om undantag i enskilda fall. Regeringen kan även överlåta åt tillsynsmyndighet att fatta sådana beslut. Datainspektionen har fått ett sådant bemyndigande.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om undantag också om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter. Regeringen har meddelat sådana föreskrifter bl.a. i fråga om kommuners, landstings och kommunalförbunds möjlighet att lägga ut diarier och protokoll på Internet.

För att en överföring av personuppgifter till tredje land skall vara tillåten räcker det enligt lagen inte med att de i 33 § eller 34 § angivna förutsättningarna är uppfyllda. Den behandling som överföringen utgör måste också vara tillåten enligt personuppgiftslagens övriga bestämmelser.

Den huvudsakliga förklaringen till att förbudet mot överföring av personuppgifter till tredje land kommit att kritiseras i samhällsdebatten är att förbudet antagits gälla också för utläggande av personuppgifter på Internet, varigenom stora delar av vad som ganska allmänt uppfattats som normal elektronisk kommunikation kommit att betraktas som olaglig. Som i korthet berörts ovan har denna problematik kommit i nytt ljus genom EG-domstolens avgörande den 6 november 2003 i det s.k. konfirmandlärarmålet. Domstolen framhöll att EG-direktivet utarbetades under en tid då

Internet ännu var föga utvecklat och att det inte kunde vara gemenskapslagstiftarens avsikt att förbjuda utläggandet av personuppgifter på Internet enbart av den anledningen att uppgifterna härigenom blev tillgängliga även i länder som inte har en adekvat skyddsnivå. Med stöd av EG-domstolens praxis skulle det alltså numera kunna hävdas att publicering på Internet är generellt undantaget från förbudet i 33 § personuppgiftslagen mot överföring av personuppgifter till tredje land. Den svenska lagstiftaren synes emellertid inte ha velat dra en så långtgående slutsats av EG-domstolens uttalande, se kapitel 23.

Anmälan till tillsynsmyndigheten

Enligt 36 § gäller som huvudregel att behandling av personuppgifter som är helt eller delvis automatiserad omfattas av anmälningsskyldighet. Regeringen eller den myndighet som regeringen bestämmer får dock meddela föreskrifter om undantag från anmälningsskyldigheten för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten. Sådana föreskrifter har meddelats bl.a. för behandlingar som utförs till följd av bestämmelserna i 2 kap. TF om utlämnande av allmän handling eller som utförs av arkivmyndighet till följd av bestämmelser om arkiv i lag eller förordning. Undantag från anmälningsskyldigheten gäller också behandlingar som i andra fall följer av lag eller förordning. Man behöver inte heller anmäla behandling av personuppgifter i löpande text.

Undantag från anmälningsskyldigheten gäller vidare om den personuppgiftsansvarige har utsett ett personuppgiftsombud och anmält denne till tillsynsmyndigheten (37 §).

I regeringens proposition inför personuppgiftslagens införande anfördes att tillsynsmyndighetens verksamhet borde koncentreras till att ge råd och sprida kunskap om de materiella reglerna och att utöva tillsyn över att reglerna följs (prop. 1997/98:44 s. 98). Det var därför viktigt att fullt ut utnyttja de möjligheter till undantag från anmälningsskyldigheten som dataskyddsdirektivet medgav. På det sättet borde anmälningsskyldigheten kunna begränsas till ett minimum.

Lagstiftarens intentioner att minimera anmälningsskyldigheten till ett minimum förefaller ha lyckats. I sin årsredovisning för 2003

rapporterade Datainspektionen att systemet med personuppgiftsombud hade utvecklats över all förväntan. Långt fler ombud har anmälts än vad man hade räknat med. Samtidigt uppgår antalet anmälda behandlingar av personuppgifter till en relativt låg siffra.

Obligatorisk anmälan av särskilt integritetskänsliga behandlingar

I 41 § anges att regeringen får meddela föreskrifter om att särskilt integritetskänsliga behandlingar skall anmälas till tillsynsmyndigheten för förhandskontroll tre veckor i förväg. Sådana föreskrifter har meddelats i fråga om behandling av personuppgifter om genetiska anlag som framkommit efter genetisk undersökning.

Tillsynsmyndighetens befogenheter

Bestämmelser om tillsynsmyndighetens, dvs. Datainspektionens, befogenheter finns i 43 – 47 §§ personuppgiftslagen. Dessa befogenheter innebär att Datainspektionen har rätt att på begäran få a) tillgång till de personuppgifter som behandlas, b) upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt c) tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (43 §).

Om en begäran enligt 43 § inte leder till ett tillräckligt underlag eller man konstaterar att uppgifter behandlas eller kommer att behandlas på ett olagligt sätt har Datainspektionen möjlighet att vid vite förbjuda annan behandling än lagring (44 och 45 §§). Dessförinnan skall myndigheten dock försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Om saken är brådskande får ett tillfälligt beslut om vite meddelas även utan att den personuppgiftsansvarige har fått yttra sig (46 §).

Tillsynsmyndigheten kan också ansöka hos länsrätt om att personuppgifter som behandlats på ett olagligt sätt skall utplånas om det inte är oskäligt (47 och 48 §§). I förarbetena uttalades att det ligger i sakens natur att möjligheten att ansöka om utplånande av personuppgifter bör användas bara i sådana fall där det inte genom andra åtgärder är möjligt att förena behandlingen av uppgifterna med de regler som gäller (prop. 1997/98:44 s. 104).

Skadestånd och straff

Enligt 48 § skall den personuppgiftsansvarige ersätta den registrerade för sådan skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat. Om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne, kan ersättningsskyldigheten jämkas i den utsträckning det är skäligt.

Bestämmelserna om skadestånd i personuppgiftslagen har karaktären av specialbestämmelser som tar över de allmänna skadeståndsreglerna i skadeståndslagen (1972:207). Skadeståndsansvaret omfattar personuppgiftsansvariga inom både den privata och den offentliga sektorn. Bestämmelserna innebär en rätt till ekonomisk kompensation för själva kränkningen förutom rätt till ersättning för personskada, sakskada och ren förmögenhetsskada.

De huvudsakliga sanktionerna vid överträdelse av personuppgiftslagen är, som framgått ovan, skadestånd och vite. Till böter eller fängelse i högst sex månader döms således enligt 49 § den som uppsåtligen eller av grov oaktsamhet

a) lämnar osann uppgift i information eller anmälan enligt lagen,
b) behandlar personuppgifter i strid med bestämmelserna om känsliga personuppgifter eller uppgifter om lagöverträdelser m.m.,
c) för över personuppgifter till tredje land i strid med 33–35 §§,
d) låter bli att göra en anmälan om behandling till tillsynsmyndigheten,
e) behandlar sådana personuppgifter som avses i 13 och 21 §§ i strid med 5 a § andra stycket, eller
f) i strid med 5 a § andra stycket för över personuppgifter till tredje land som inte har en sådan adekvat nivå för skyddet av personuppgifterna som avses i 33 §.

Om brottet är grovt är straffet fängelse i högst två år. Från och med den 1 januari 2000 är inte längre gärningar som utgör ringa brott straffbara. Ändringen hade samband med den tidigare redovisade ”uppmjukningen” av förbudet mot överföring av personuppgifter till tredje land.

Överklagande

Enligt 51 § får tillsynsmyndighetens beslut enligt personuppgiftslagen överklagas hos allmän förvaltningsdomstol.

4.5.4 Avkriminalisering och avreglering när personuppgifter behandlas i löpande text m.m.

Den 1 januari 2007 trädde ändringar i personuppgiftslagen i kraft som syftade till att underlätta behandling av personuppgifter i löpande text och annat ostrukturerat material (prop. 2005/06:173, bet. 2005/06:KU37). Ändringarna innebar bl.a. att det i en ny paragraf – 5 a § – införts bestämmelser om att behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter inte omfattas av flertalet av de hanteringsregler som anges i personuppgiftslagen. Det som i stället avgör om en sådan behandling är tillåten eller inte är huruvida behandlingen innebär en kränkning av den registrerades personliga integritet, dvs. en s.k. missbruksmodell skall tillämpas.

Att hanteringsreglerna inte behöver tillämpas på behandling av personuppgifter i t.ex. löpande text innebär att den som behandlar uppgifterna inte behöver beakta bestämmelserna om grundläggande krav på behandlingen (9 §) eller om när behandling av uppgifter är tillåten (10 §). Inte heller behöver förbuden mot att behandla känsliga personuppgifter (13 §) eller uppgifter om lagöverträdelser m.m. (21 §) iakttas eller de särskilda villkoren för behandling av personnummer (22 §) beaktas. Bestämmelserna om skyldighet att lämna information behöver inte tillämpas (23, 24 och 26 §§). Rättelse av uppgifter behöver inte heller vidtas (28 §) och förbudet mot överföring av personuppgifter till tredje land behöver inte iakttas (33 §).

I förarbetena anfördes (prop. 2005/06:173 s. 19) att även behandling av personuppgifter i ett ostrukturerat material kan innebära en kränkning av den av personliga integriteten eller medföra risk för en sådan kränkning i ett enskilt fall. Vid behandling av personuppgifter som inte finns i en tydligt personuppgiftsanknuten registerstruktur framstod emellertid enligt regeringen hanteringsreglerna som alltför omfattande och

byråkratiska med hänsyn bl.a. till att integritetsriskerna normalt är mindre och till de informations- och yttrandefrihetsintressen som gör sig gällande. Som både utredningen och en del remissinstanser framhållit var det heller inte realistiskt att tro att hanteringsreglerna i praktiken tillämpas i någon större utsträckning vid vardaglig, ostrukturerad hantering av personuppgifter. Man riskerade därmed att de grundläggande och viktiga dataskyddsprinciperna råkar i vanrykte och inte tillämpas ens vid sådan strukturerad behandling av personuppgifter där de är nödvändiga för integritetsskyddet. Mot bakgrund av detta skulle enligt regeringen integritetsskyddet i praktiken stärkas om man undantog typiskt sett mindre riskfylld behandling från hanteringsreglernas tillämpningsområde och i stället skapade enklare regler som direkt tar sikte på skydd mot missbruk av personuppgifter.

Lagrådet ansåg det problematiskt att den nya, allmänt hållna regeln i 5 a § inrymde uttryck som måste antas ge upphov till tillämpningssvårigheter. Regeringen delade inte denna bedömning, utan ansåg att regeln inte kommer att medföra påtagliga problem från rättssäkerhetssynpunkt, även om gränsdragningen i vissa enskilda fall inte kommer att vara självklar (a. prop. s. 20 f.). De behandlingar som omfattas av den nya missbruksregeln var enligt regeringen sammanfattningsvis vardaglig hantering som produktion av löpande text i ordbehandlingsprogram, publicering av löpande text på Internet, användning av ljud- och bildupptagningar och korrespondens med e-post under förutsättning att materialet inte ingår i eller skall infogas i en databas med en personuppgiftsanknuten struktur såsom ett ärendehanteringssystem. Vill man infoga materialet i någon form av databas blir frågan om databasen har en personuppgiftsanknuten struktur avgörande. Om så är fallet, måste hanteringsreglerna tillämpas.

När det gäller frågan om när en behandling av personuppgifter i ostrukturerat material innebär en kränkning av den registrerades personliga integritet anförde regeringen att det ligger i sakens natur att tillämpningen av missbruksregeln får bygga på en intresseavvägning, där den registrerades intresse av en fredad, privat sfär vägs mot andra motstående intressen i det enskilda fallet (a. prop. s. 27 f.). Enligt regeringen låg detta också i linje med vad EG-domstolen uttalat i det s.k. konfirmandlärarmålet om att det åligger de nationella myndigheterna och domstolarna att vid en tolkning av de bestämmelser som genomför EG-direktivet i nationell lagstiftning göra en avvägning mellan olika intressen och inte

grunda sig på en tolkning som skulle i strid med bl.a. de grundläggande rättigheter som skyddas genom gemenskapernas rättsordning.

Bedömningen av vad som är en kränkning skall alltså inte göras schablonartat enbart utifrån vilka uppgifter som behandlas utan måste även ta sin utgångspunkt i t.ex. vilket sammanhang uppgifterna förekommer, för vilket syfte de behandlas, vilken spridning de har fått eller har riskerat att få samt vad behandlingen kan leda till. Om uppgifter samlas in eller annars behandlas med syfte att förfölja eller skandalisera en person, får behandlingen anses innebära en kränkning av den personliga integriteten. Regeringen anförde vidare att en enskild person ofta torde ha rätt att kräva att ingen har en i det närmaste fullständig kunskap om honom eller henne. Redan det förhållandet att en personuppgiftsansvarig samlar en stor mängd uppgifter om en person utan något godtagbart ändamål måste därför ses som en kränkning av den personliga integriteten. Vidare får det oftast anses innebära en kränkning av den registrerades personliga integritet om den personuppgiftsansvarige medvetet behandlar personuppgifter som är klart felaktiga eller missvisande.

Regeringen ansåg att det inte behövdes några särskilda regler till skydd mot angrepp på heder och ära vid just automatiserad behandling av personuppgifter i ostrukturerat material, utan de befintliga reglerna om förtal och förolämpning var tillräckliga även i detta sammanhang (a. prop. s. 28). När det gällde spridning av förtroliga eller djupt personliga uppgifter fanns det enligt regeringen redan i viss utsträckning författningsbestämmelser och etiska regler eller motsvarande som föreskriver tystnadsplikt i fråga t.ex. om uppgifter om personliga förhållanden. Dessa regler kunde sägas ge uttryck för vilka förhållanden som bör hemlighållas. En spridning av personuppgifter som innebär brott mot sådana bestämmelser och riktlinjer borde i de flesta fall anses utgöra en kränkning av den personliga integriteten i missbruksregelns mening.

Vid samma tillfälle gjordes också en avkriminalisering vid behandling av personuppgifter på så sätt att gärningar som begås av oaktsamhet inte längre skall vara straffbara, utan bara uppsåtliga eller grovt oaktsamma förfaranden. I förarbetena påpekades att den oaktsamhet som den personuppgiftsansvarige uppvisat, t.ex. i förhållande till om behandlingen utförts i ett ostrukturerat material eller till att känsliga personuppgifter har behandlats, kan i det

enskilda fallet vara mindre klandervärd (a. prop. s. 47 f.). En avkriminalisering av oaktsamhet av normalgraden skulle i sådana fall motverka oskäliga resultat. Detta gäller både för det område som faller in under missbruksregeln och det som fortfarande regleras av hanteringsreglerna.

4.5.5 Sekretess för personuppgifter

I 7 kap. 16 § SekrL (1980:100) finns ett allmänt sekretesskydd för personuppgifter, vilket träder i funktion om det kan antas att ett utlämnande skulle medföra att uppgifterna behandlas i strid med personuppgiftslagen. Bestämmelsen har ersatt en motsvarande bestämmelse i sekretesslagen som refererade till datalagen (1973:289). När bestämmelsen infördes, vilket skedde i samband med att personuppgiftslagen ersatte datalagen, uttalades i förarbetena att ändringen endast innebar en samordning med bestämmelserna i personuppgiftslagen (prop. 1997/98:44 s. 147).

Emellertid har den ändrade bestämmelsen kommit att få ett vidare tillämpningsområde än tidigare och sekretessprövningen har blivit mer komplicerad (se betänkandet *Offentlighetsprincipen och den nya tekniken* SOU 2001:3 s. 190 f. och 213 f. samt *Översyn av personuppgiftslagen* SOU 2004:6 s. 253). Bestämmelsen skall numera tillämpas vid alla utlämnanden av personuppgifter från en myndighet och inte enbart vid utlämnanden från myndigheternas personregister. Den omständigheten att sekretessprövningen numera tar sikte på personuppgiftslagens bestämmelser och inte reglerna i datalagen innebär också att tillämpningsområdet blivit vidare. Personuppgiftslagen omfattar ju all helt eller delvis automatiserad behandling av personuppgifter samt behandling i manuella register, medan datalagen enbart omfattade behandling av personuppgifter i dataregister.

Regleringen i datalagen byggde på ett system där inrättande och förande av personregister förutsatte licens från Datainspektionen. Därutöver krävdes tillstånd för vissa typer av känsliga personregister. Systemet med licens och tillståndsprövning innebar att sekretessprövningen enligt dåvarande 7 kap. 16 § i flertalet fall kunde inskränkas till ett konstaterande av huruvida den sökande hade licens eller tillstånd av Datainspektionen för det aktuella personregistret. Som framgått ovan bygger personuppgiftslagens regler i stället på ett system med anmälningsskyldighet, som är

förenat med tämligen vittgående undantag. Detta system innebär att den myndighet som skall pröva om sekretess enligt 7 kap. 16 § föreligger har att på egen hand ta ställning till om den behandling som de begärda uppgifterna skall användas till är förenlig med bestämmelserna i personuppgiftslagen.

Ändringen av 7 kap. 16 § har medfört ett ökat antal mål i förvaltningsdomstolarna som rör tillämpningen av bestämmelsen. Det har också hunnit avgöras ett antal mål i högsta instans. En viss rättspraxis har således hunnit utbildas sedan bestämmelsen i dess nya lydelse trädde i kraft (för en redovisning av praxis, se SOU 2004:6 s. 62 f.).

Den ändring i lydelsen av 7 kap. 16 § SekrL som gjordes i samband med personuppgiftslagens införande innebar vidare att ett andra stycke i paragrafen upphävdes. I detta stycke angavs vad som gällde i fråga om sekretess vid utlämnande av personuppgifter i personregister till utlandet. Motivet för att upphäva det andra stycket var att det i 33–35 §§ personuppgiftslagen finns bestämmelser om överföring av personuppgifter till tredje land som gäller även för myndigheter (prop. 1997/98:44 s. 147). I förarbetena erinrades om att redan första stycket i 7 kap. 16 § innebär att sekretess gäller om ett utlämnande av personuppgifter till tredje land skulle stå i strid med de nämnda bestämmelserna i personuppgiftslagen. Andra stycket i paragrafen behövdes därför inte längre.

Lagstiftaren tycks emellertid ha blandat samman vilken behandling av personuppgifter det är som skall prövas mot bestämmelserna i personuppgiftslagen. Är det den behandling som myndighetens utlämnande innebär som skall prövas, eller är det frågan om den behandling som kan antas ske efter utlämnandet? Att det enbart är sökandens efterföljande behandling som avses får numera anses klarlagt genom den rättspraxis som kommit till efter ändringen (SOU 2004:6 s. 62 f. och 252). Hur 7 kap. 16 § i sin ändrade lydelse skall tillämpas vid begäran om utlämnande till en sökande som befinner sig utanför personuppgiftslagens territoriella tillämpningsområde har inte prövats, åtminstone inte i de högre rättsinstanserna.

5 Skatteområdet

Huvudsaklig bedömning:

– Det har i lagstiftningen inte lämnats någon godtagbar förklaring till att möjligheterna att lämna ut uppgifter till andra myndigheter måste vara mycket större på skatteområdet än vad som är fallet på andra områden där absolut sekretess gäller.
– Bestämmelserna om att skattebrottsenheterna inom Skatteverket skall ha direktåtkomst till beskattningsdatabasen har införts utan att en tillräcklig redovisning och analys har gjorts av behovet av en sådan åtkomst och dess effektivitet å ena sidan och konsekvenserna för integritetsskyddet å andra sidan. Någon avvägning mellan behov och konsekvenser för integritetsskyddet har därför inte varit möjlig att göra. Även detta förhållande är otillfredsställande från integritetsskyddssynpunkt.

5.1 Allmänt om skatteområdet

Den 1 januari 2004 bildade Riksskatteverket och landets tio regionala skattemyndigheter den nya myndigheten Skatteverket. Skatteverket är en sammanhållen myndighet med hela landet som verksamhetsområde. De regionala skattemyndigheterna har därmed upphört. Skatteverket är därtill chefsmyndighet för exekutionsväsendet.

Skatteverkets huvuduppgift är att administrera stora delar av det svenska skattesystemet. Dessutom ansvarar Skatteverket för bl.a. folkbokföring, fastighetstaxering och registrering av bouppteckningar. Skatteverket medverkar även i brottsutredningar. Denna verksamhet bedrivs av en särskild enhet inom Skatteverket och är att betrakta som en självständig verksamhetsgren i förhållande till beskattningsverksamheten. En annan uppgift för

Skatteverket är att företräda staten vid domstol. Sedan den 1 januari 2005 är Skatteverket värdmyndighet för SPAR-nämnden, som ansvarar för statens person- och adressregister.

5.2 Kort om regelverket

5.2.1 Sekretess

I 9 kap. 1 och 2 §§ SekrL finns regler om sekretess till skydd för enskildas personliga och ekonomiska förhållanden i Skatteverkets *beskattningsverksamhet*. Sekretessen omfattar såväl taxeringsärendena som registerföring och annan verksamhet som har anknytning till taxeringsförfarandet. Den omfattar också Skatteverkets brottsbekämpande verksamhet. Även uppgiften att företräda det allmänna som part i skatteprocess i domstol faller in under sådan verksamhet som omfattas av sekretess.

Sekretessen är *absolut*, dvs. något skaderekvisit finns inte. Ett undantag är skatteprocess hos domstol, där sekretess gäller med ett rakt skaderekvisit för uppgift i mål hos domstolen. I en skatteprocess i domstol gäller alltså presumtion för offentlighet.

För den del av Skatteverkets verksamhet som avser att ansvara för folkbokföringen finns bestämmelser om sekretess i 7 kap. 15 § SekrL. Förutsättningen för sekretess är att det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs, dvs. det är fråga om ett rakt skaderekvisit som innebär presumtion för offentlighet. Denna sekretess är också tillämplig på uppgifter i det statliga person- och adresseregistret (SPAR).

Sekretess i skatteverkets *brottsbekämpande verksamhet* regleras i 9 kap. 17 § SekrL, där bestämmelser finns om s.k. förundersökningssekretess. Sådan sekretess gäller med omvänt skaderekvisit, dvs. med presumtion för sekretess, och gäller förutom i förundersökning i brottmål också i Skatteverkets verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott. Denna sekretess omfattar också den behandling av personuppgifter som sker inom ramen för den brottsbekämpande verksamheten.

Även om det råder absolut sekretess i beskattningsverksamheten för uppgifter om enskilds personliga förhållanden innebär sekretessen inget hinder mot att lämna ut uppgifter till en annan myndighet i de fall det i lag eller förordning har föreskrivits en

uppgiftsskyldighet. Detta följer av 14 kap. 1 § SekrL, där det föreskrivs att sekretess inte hindrar att uppgift lämnas till annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Både genom lag och förordning har föreskrivits en ganska omfattande uppgiftsskyldighet för skattemyndigheterna. Bestämmelser om uppgiftsskyldighet i förhållande till andra myndigheter finns i 4–8 §§ förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

Trots att det råder absolut sekretess i Skatteverkets beskattningsverksamhet har sekretessen inte ansetts hindra att uppgifter lämnas till andra myndigheter med stöd av 14 kap. 3 § SekrL. Enligt denna bestämmelse *får* sekretessbelagd uppgift lämnas till myndighet – dvs. trots att någon uppgiftsskyldighet inte är föreskriven i lag eller förordning – om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen skall skydda.

I 9 kap. 1 § anges också vissa undantag från den absoluta sekretessen. Det gäller för det första beslut om skatt eller pensionsgrundande inkomst (9 kap. 1 § tredje stycket). Det har också ansetts nödvändigt att ge möjlighet för ett visst uppgiftsutlämnande till enskilda. Detta innebär bl.a. att uppgifter utan hinder av sekretess kan lämnas till enskilda enligt vad som föreskrivs i lag om förfarandet vid beskattning, i lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet eller i lagen (1990:613) om miljöavgift på utsläpp av kväveoxider vid energiproduktion. Även t.ex. uppgifter i ärenden om revision får lämnas ut till förvaltaren i den reviderades konkurs.

En mer utförlig redovisning av sekretessreglerna på skatteområdet lämnas i kapitel 25.

5.2.2 Behandling av personuppgifter

Under år 2001 antogs fem nya lagar som led i en reform av författningsregleringen när det gäller behandlingen av personuppgifter inom Skatteverkets verksamhet, de dåvarande kronofogdemyndigheternas verksamhet och Tullverkets verksamhet med att uppbära tullar m.m. En reform på området ansågs behövlig med hänsyn till den snabba utvecklingen av datoriseringen inom myndighetsområdet. Inom de nu aktuella myndigheternas verksamhet hade Tullverket hunnit längst i sin datorisering genom

att ha rationaliserat bort en stor del av pappershanteringen. Även inom skatteförvaltningen hade pågått projekt med syfte att i allt högre grad automatisera den i stora delar redan automatiserade ärendehanteringen. Inom exekutionsväsendet hade man inte ännu inte kommit lika långt, men på sikt planerade man införa en i stort sett helt elektronisk ärendehantering. Behov av en författningsreform fanns också med anledning av att EG:s dataskyddsdirektiv hade antagits år 1995 och införlivats med svensk lagstiftning genom personuppgiftslagen år 1998.

En allmän utgångspunkt vid reformen var att de grundläggande principerna för att skydda den enskildes integritet borde regleras i lag medan frågor som inte var centrala från integritetssynpunkt i stället borde regleras i förordning (prop. 2000/01:33 s. 84 f.). I lagen borde därför klart anges för vilka ändamål uppgifter får behandlas. Dessutom borde anges de yttre ramarna för vad registren skulle få innehålla. I lag skulle också anges de begränsningar som skulle gälla för behandling av uppgifter vid direktåtkomst och utlämnande av uppgifter till enskilda. Även frågor om personuppgiftsansvar och därmed sammanhängande frågor borde regleras i lag.

De nya författningarna skulle omfatta all automatiserad behandling av personuppgifter samt i vissa fall behandling av uppgifter som kunde hänföras endast till juridiska personer eller avlidna. Behandling av personuppgifter i administrativ verksamhet skulle inte omfattas, utan för sådan verksamhet skulle personuppgiftslagens regler gälla fullt ut.

En annan allmän utgångspunkt vid reformen var att det skulle särskilt anges i de nya lagarna vilka bestämmelser i personuppgiftslagen som skulle tillämpas. En sådan lagstiftningsteknik för att beskriva en specialförfattnings förhållande till personuppgiftslagen kritiserades av Lagrådet vid lagarnas införande (a. prop. s. 345). Lagrådet ansåg lagstiftningstekniken otillfredställande och samtidigt riskfylld, med hänsyn såväl till svårigheterna att överblicka om dataskyddsdirektivet blir till fullo genomfört i registerlagarna som till risken att vid kommande lagändringar hänvisningar till personuppgiftslagen blir felaktiga eller ofullständiga. Regeringen ansåg dock, med instämmande av riksdagen, att metoden skulle tillämpas med motivering att lagen på så sätt blir överskådlig och tydlig för tillämparen (a. prop. s. 88).

Slutligen skulle begreppet databas införas som en juridisk beteckning på vissa fastställda automatiserade uppgiftssamlingar

som används gemensamt inom en verksamhet och för vilka särskilda regler skulle gälla.

Vid reformen infördes lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet. Lagen ersatte den tidigare skatteregisterlagen (1980:343).

Vid reformen antogs också lagen (2001:182) om behandling av uppgifter i Skatteverkets folkbokföringsverksamhet, som ersatte lagen (1990:1536) om folkbokföringsregister och lagen (1995:743) om aviseringsregister.

Behandling av personuppgifter i Skatteverkets brottsbekämpande verksamhet sker med stöd av lagen (1990:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar. Denna lag har inte samma uppbyggnad som de andra lagarna på skatteområdet, utan har disponerats på samma sätt som polisdatalagen (1998:622).

Även för behandlingen av personuppgifter i SPAR-registret finns en särskild författning, lagen (1998:527) om det statliga personadressregistret.

En utförlig redovisning av bestämmelserna om behandling av personuppgifter på skatteområdet lämnas i kapitel 25.

5.2.3 Nya regler för en effektivare skattekontroll

Den 1 juli 2006 trädde ändringar i lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar i kraft (prop. 2005/06:169, bet. 2005/06:SkU29). Ändringarna innebar att utredare vid Skatteverkets skattebrottsenheter har getts en lagstadgad rätt att medverka vid husrannsakningar och aktivt söka efter handlingar. Dessa utredare har också rätt att, efter beslut av åklagare, ta handlingar i beslag i den mån våld mot person inte behöver användas.

Vid samma reform medgavs skattebrottsenheterna även en mer omfattande direktåtkomst till uppgifter i beskattningsdatabasen. Reformen i denna del föranledde ändringar i lagen (1990:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt i lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet. I den sistnämnda lagen har i 1 kap. 4 §, som reglerar för vilka ändamål hos Skatteverket som uppgifter får behandlas, införts ett nytt andra stycke. I detta stycke föreskrivs att uppgifter som får behandlas enligt första stycket även får behandlas för tillhandahållande av information som

behövs i Skatteverkets brottsbekämpande verksamhet enligt lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar. Denna bestämmelse har kompletterats med en ny paragraf – 5 a § – i förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet, i vilken sägs att vissa uppgifter som avses i lagen om behandling av personuppgifter i Skatteverkets beskattningsverksamhet skall på begäran lämnas ut till en enhet inom Skatteverket som medverkar vid brottsutredningar. Det är alltså frågan om en sådan uppgiftsskyldighet som bryter sekretess i enlighet med 14 kap. 1 § SekrL.

När det gällde skattebrottsenheternas behov av direktåtkomst till beskattningsdatabasen anfördes i förarbetena att i fråga om underrättelseverksamheten var tidsutdräkten den största nackdelen med att inte ha direktåtkomst (prop. 2005/06:169 s. 80 f.). Beträffande den brottsutredande verksamheten anfördes att behovet hade sin grund i svårigheten att överblicka vilka uppgifter ur beskattningsdatabasen som behövdes i den aktuella utredningen, vilket kunde innebära att man ibland måste göra fler förfrågningar. Sammanfattningsvis konstaterade regeringen att behovet av direktåtkomst var mindre i den brottsutredande verksamheten än i underrättelseverksamheten, men att det tveklöst var så att direktåtkomst skulle effektivisera skattebrottsenheternas verksamhet även inom detta område.

I fråga om skyddet för den personliga integriteten anförde regeringen att de uppgifter som efterfrågas av skattebrottsenheterna ofta rör uppgifter om juridiska personer. När det gällde uppgifter om fysiska personer var uppgiftsbehovet nästan uteslutande hänförligt till näringsverksamhet. Under förutsättning att det finns författningsreglerade integritetsskyddande begränsningar av den brottsbekämpande verksamhetens möjligheter att använda sig av åtkomsten ansåg regeringen att risken för integritetskränkningar fick anses vara väl uppvägd av de effektivitetsvinster som skulle uppnås i den brottsbekämpande verksamheten. Genom att låta direktåtkomsten omfatta särskilt utvalda och typiskt sett något mindre integritetskänsliga uppgifter kunde risken för integritetsintrång enligt regeringen minskas. Skattebrottsenheternas behov av uppgifter som rör planerad, pågående eller avslutad revision samt yrkanden, grunder och beslut i ett ärende var dock så stort att direktåtkomst borde tillåtas även om det var fråga om uppgifter som är att betrakta som känsliga ur integritetssynpunkt. Någon inskränkning skulle inte heller göras till personer som är

misstänkta för ett konkret brott eller för brottslig verksamhet, utan därvid borde de allmänna bestämmelserna om behandling av personuppgifter utgöra ett tillräckligt skydd.

Regeringen konstaterade vidare att bestämmelserna i 14 kap. SekrL om uppgiftsutbyte mellan myndigheterna och om uppgiftsskyldighet i skattebrottslagen (1971:69) ger ett visst utrymme för uppgiftslämnande från den fiskala verksamheten till den brottsbekämpande verksamheten. För att säkerställa skattebrottsenheternas möjligheter till direktåtkomst till beskattningsdatabasen borde dock en sekretessbrytande regel införas. Detta borde ske i förordningsform. Någon sekretessprövning skulle därmed inte längre behöva göras vid utlämnande av uppgifter.

5.3 Sammanfattning och bedömning

5.3.1 Betydelsen av absolut sekretess vid utlämnande av uppgifter till andra myndigheter

Enligt 9 kap. 1 § SekrL råder absolut sekretess för uppgift om enskilds personliga förhållanden i Skatteverkets beskattningsverksamhet. Som skäl för denna stränga form av sekretess har bl.a. åberopats den skattskyldigas långtgående plikt att lämna uppgifter om sina förhållanden (prop. 1979/80:2 Del A, s. 256 f.).

När det gäller utlämnande av uppgifter till enskilda innebär absolut sekretess att uppgifter bara kan lämna ut i de fall det är särskilt föreskrivet att sådant utlämnande är tillåtet. I fråga om beskattningsverksamheten finns ett sådant undantag i 9 kap. 1 § femte stycket SekrL.

Beträffande utlämnande till andra myndigheter finns bestämmelser i 14 kap. SekrL som medger sådant uppgiftsutbyte. I 14 kap. 1 § sägs att sekretess inte hindrar att uppgift lämnas till annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Vidare finns i 14 kap. 2 § SekrL bestämmelser som innebär möjligheter att under vissa förutsättningar lämna ut uppgifter till brottsbekämpande myndigheter. Därutöver gäller enligt den s.k. generalklausulen i 14 kap. 3 § första stycket SekrL att sekretessbelagd uppgift som huvudregel får lämnas till myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen skall skydda. I förarbetena har sagts att om uppgiftsutbytet mellan myndigheter är avsett att bli

rutinmässigt måste den intresseavvägning som skall göras ske på förhand och den behöver inte avse prövning av individuella fall. Helst bör det rutinmässiga uppgiftslämnandet vara författningsreglerat. Bedömningen kan därvid göras på ett sätt som liknar den som skall ske i fråga om massuttag (prop. 1979/80:2 Del A s. 327, jfr s. 81). Har det i lag eller förordning föreskrivits att en uppgift ”bör” eller ”får” lämnas ut talar detta för att generalklausulen är tillämplig (Regner m.fl., a.a., s. 14:27).

Om absolut sekretess gäller inom ett område för uppgift om enskilds personliga förhållanden brukar möjligheten att lämna ut uppgifter inte vara begränsad bara i förhållande till enskilda, utan också i förhållande till andra myndigheter. Så är fallet i fråga om uppgifter i belastningsregistret, där tillämpning av hela 14 kap. SekrL är undantagen (7 kap. 17 §). När det gäller uppgifter i statistisk verksamhet och i postverksamhet gäller mer begränsade möjligheter än för andra myndigheter att lämna ut uppgifter om brottsmisstankar till brottsbekämpande myndigheter (14 kap. 2 § femte stycket). Vidare är uppgiftsutbyte enligt den s.k. generalklausulen i 14 kap. 3 § inte tillåtet (14 kap. 3 § andra stycket). I stället har särskilt reglerats genom undantag i sekretesslagen när utlämnande får ske.

Några begränsningar i möjligheterna att lämna ut uppgifter vare sig till brottsbekämpande myndigheter eller till andra myndigheter enligt 14 kap. gäller dock inte för Skatteverket, trots att det även på detta område gäller absolut sekretess. Lagstiftaren har sålunda ansett att möjligheterna att lämna ut uppgifter till andra myndigheter skall vara mycket större på skatteområdet än vad som är fallet på andra områden där absolut sekretess gäller. I förhållande till vad som gäller på övriga områden med absolut sekretess, ger regleringen av sekretesskyddet på skatteområdet därför intryck av viss inkonsekvens. Från integritetsskyddssynpunkt kan det inte anses tillfredsställande att den absoluta sekretessen har en annan innebörd på skatteområdet än på andra områden.

5.3.2 Förhållandet mellan skattesekretessen och regler om behandling av personuppgifter

Som nämnts ovan har det ansetts möjligt att lämna ut uppgifter från Skatteverkets beskattningsverksamhet med stöd av den s.k. generalklausulen i 14 kap. 3 §, trots att där gäller absolut sekretess.

Om det i lag eller förordning föreskrivits att en uppgift ”bör” eller ”får” lämnas ut har detta ansetts tala för att generalklausulen är tillämplig. Av stor betydelse blir därför *om* och *hur* frågan om utlämnande av uppgifter har reglerats i författning.

När det gäller frågan om hur förhållandet mellan sekretess å ena sidan och behandling av personuppgifter å andra sidan kan beskrivas och hur detta förhållande kan komma till uttryck i föreskrifter som rör utlämnande av uppgifter om enskilda personer kan följande reflektioner göras beträffande skatteområdet. I de aktuella databaslagarna, som infördes genom lagstiftningsreformen på området för skatt och exekution, har förhållandet mellan sekretess och tillåten behandling av personuppgifter – i form av utlämnande av uppgifter – inte kommit till uttryck i lagtexten eller kommenterats i förarbetena. Lagrådet hade synpunkter på hur lagtexten hade formulerats i reglerna om direktåtkomst (prop. 2000/01:33 s. 344 f.). Även om de aktuella reglerna i fråga om Skatteverkets beskattningsverksamhet och kronofogdemyndigheterna avsågs ha en sekretessbrytande funktion, dvs. innebära en sådan uppgiftsskyldighet som avses i 14 kap. 1 § SekrL, hade orden ”får ha direktåtkomst” använts i förslagen till lagtext. Lagrådet ansåg att orden ”skall ha” i stället borde användas för att markera vilken verkan bestämmelserna avsågs få på sekretessen. Regeringen – och riksdagen – följde emellertid inte dessa synpunkter, utan ansåg att det var mer ändamålsenligt att i en förordning ta in de sekretessbrytande bestämmelser som behövs för utlämnande genom direktåtkomst.

I förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet, som trädde i kraft samma dag som lagen om behandling av uppgifter i skatteverkets beskattningsverksamhet, har ännu inte meddelats några föreskrifter om myndigheters direktåtkomst till beskattningsdatabasen. Däremot finns i förordningen bestämmelser om Skatteverkets uppgiftsskyldighet i förhållande till ett antal myndigheter (4–8 §§). Dessa bestämmelser reglerar inte på vilket sätt uppgifter skall lämnas ut, utan föreskriver enbart att de *skall* lämnas ut på begäran av respektive myndighet. Liknande bestämmelser om uppgiftsskyldighet finns i förordningen (2001:590) om behandling av uppgifter i Kronofogdemyndighetens verksamhet (7 och 8 §§). Vid sådant förhållande får inte uttrycket ”får ha direktåtkomst” i de nämnda databaslagarna någon effekt på sekretessen, utan torde närmast betyda att Skatteverket förfogar över den mer praktiska frågan

huruvida utlämnandet av uppgifter till de aktuella myndigheterna skall ske genom direktåtkomst eller inte (dock förfogar Skatteverket inte över frågan *vilka* myndigheter som skall medges direktåtkomst). Att det förhåller sig på detta sätt kan emellertid inte utläsas av databaslagarna, eftersom där inte framgår att Skatteverket och Kronofogdemyndigheten har uppgiftskyldighet i förhållande till vissa myndigheter. Databaslagarnas regler om direktåtkomst ger i stället intryck av att sådan åtkomst – genom ordvalet ”får ha” – kan medges först efter en sådan intresseavvägning mellan behovs- och skyddsintressen som avses i 14 kap. 3 § SekrL.

Den sekretessbrytande uppgiftsskyldighet som i förordning finns föreskriven för Skatteverket i förhållande till vissa myndigheter har inte heller kommit till tydligt uttryck vare sig i bestämmelserna om ändamål med behandlingen av uppgifter eller i förarbetsuttalandena som rör dessa bestämmelser. Behandling för tillhandahållande av information till andra myndigheter regleras i bestämmelser om ”sekundära ändamål”. Där görs ingen skillnad på om fråga är om tillhandahållande på grund av uppgiftsskyldighet eller efter en sådan prövning som avses i 14 kap. 3 § SekrL, eller om det rentav är fråga om utlämnande av offentliga uppgifter. När det gäller bestämmelserna om sekundära ändamål kan det också synas egendomligt att det inte framgår av förarbetena hur de är avsedda att förhålla sig till bestämmelsen i 14 kap. 3 § SekrL, t.ex. om de avser att utgöra vägledning vid en avvägning mellan skydds- och behovsintressen enligt nämnda bestämmelse eller om de förutsätter att myndigheten redan har konstaterat att sekretess inte utgör hinder för ett uppgiftsutlämnande. Som påpekats ovan har det ansetts att föreskrifter i lag eller förordning om att uppgifter ”får” lämnas ut, talar för att 14 kap. 3 § SekrL är tillämplig.

Sammanfattningsvis kan sägas att det är angeläget att bestämmelser om behandling av personuppgifter som tar sikte på eller får återverkan på frågan om utlämnande av uppgifter är tydliga när det gäller hur bestämmelserna förhåller sig till regler om sekretess. I synnerhet är detta viktigt på ett område som beskattningsverksamheten där det råder absolut sekretess.

Frågan om hur bestämmelser om behandling av personuppgifter i personuppgiftslagen (1998:204) eller i annan lag förhåller sig till sekretesslagens regler har befunnits utgöra ett problem vid rättstillämpningen. Som redovisats ovan ansåg Lagrådet att det var önskvärt att en formell överensstämmelse erhölls mellan registerlagar och sekretesslagen så att de sekretessbrytande effekterna av före-

skrifter om direktåtkomst regleras i sekretesslagen i anslutning till 14 kap. 1 och 3 §§. Offentlighets- och sekretesskommittén har i sitt betänkande *Ny sekretesslag* (SOU 2003:99 s. 230 f.) behandlat frågan hur sekretesslagens bestämmelser om uppgiftsutbyte mellan myndigheter förhåller sig till den i personuppgiftslagen uttryckta s.k. finalitetsprincipen, som innebär att uppgifter inte får behandlas för ett ändamål som är oförenligt med det ändamål för vilket de samlats in. Enligt Offentlighets- och sekretesskommittén har man i sekretessbestämmelserna som reglerar uppgiftsutbyte mellan myndigheter redan tagit hänsyn till integritetsaspekterna. De utlämnanden av personuppgifter till en annan myndighet som sker i överensstämmelse med sekretesslagen borde därför vara att anse som en tillåten behandling enligt personuppgiftslagens bestämmelser. För att undanröja oklarheterna härvidlag borde enligt Offentlighets- och sekretesskommittén en särskild bestämmelse införas i personuppgiftslagen av innebörd att bestämmelser i den lagen inte hindrar att en myndighet lämnar en personuppgift till en annan myndighet, om utlämnandet sker i överensstämmelse med sekretesslagen.

Någon sådan bestämmelse har emellertid inte införts, varför de påtalade oklarheterna med åtföljande risker för integritetsskyddsförluster kvarstår.

5.3.3 Skattebrottsenheterna direktåtkomst till beskattningsdatabasen

Från och med den 1 juli 2006 har skattebrottsenheterna inom Skatteverket direktåtkomst till beskattningsdatabasen. Beskrivningen i förarbetena (prop. 2005/06:129) av behoven av en sådan direktåtkomst får anses mycket knapphändig. Behoven synes inte hänföra sig till att det utan sådan åtkomst skulle vara omöjligt att få tillgång till uppgifter i beskattningsdatabasen, utan att uppgifter annars kan erhållas först efter en viss tidsutdräkt och att omfrågningar kan bli nödvändiga.

I förarbetena har inte heller annat än översiktligt redovisats vilken effektivitet som kan uppnås med en direktåtkomst. Regeringen konstaterade att bestämmelserna i 14 kap. SekrL och om uppgiftsskyldighet i skattebrottslagen gav utrymme för ett visst uppgiftsutlämnande från beskattningsverksamheten till de brottsbekämpande enheterna inom Skatteverket. En sekretessbrytande

regel borde likväl införas för att säkerställa åtkomsten till uppgifterna i beskattningsdatabasen. Vilka möjligheter gällande regler gav när det gällde uppgiftsutlämnande varken redovisades eller analyseras på något mer ingående sätt. Därmed var det inte möjligt att bedöma effektiviteten av en direktåtkomst, som ju innebär att uppgifter kan lämnas ut utan att någon sekretessprövning sker.

Vad skattebrottsenheternas direktåtkomst till beskattningsdatabasen får för konsekvenser för integritetsskyddet har på ett mycket knapphändigt sätt analyserats i förarbetena. Den principiellt viktiga frågan om vad det innebär från integritetsskyddssynpunkt att man ger en brottsbekämpande myndighet tillgång till uppgifter från en verksamhet som har ett helt annat syfte samtidigt som den enskilde är skyldig att lämna in uppgifter om sina personliga och ekonomiska förhållanden, diskuterades över huvud taget inte. Inte heller behandlades den från rättssäkerhetssynpunkt viktiga frågan huruvida en sådan åtkomst är förenlig med artikel 6 i Europakonventionen om rätten till en rättvis rättegång, vari har ansetts ligga en ”passivitetsrätt”. Den misstänkte skall enligt denna princip inte behöva bidra till utredningen eller bevisningen i målet genom att göra medgivanden eller tillhandahålla belastande material (jfr avsnitt 14.3.5 om uppgiftsutbyte inom Tullverket). Det kan vidare konstateras att direktåtkomsten inte har avgränsats till att gälla personer som är misstänkta för att ha begått ett brott eller för att delta i brottslig verksamhet. Eftersom det i Skatteverkets brottsbekämpande verksamhet gäller sekretess med ett omvänt skaderekvisit (9 kap. 17 § första stycket 8 SekrL), får de uppgifter som hämtas till den brottsbekämpande verksamheten ett sämre sekretesskydd än de hade i beskattningsverksamheten.

Sammanfattningvis kan alltså konstateras att bestämmelserna om att skattebrottsenheterna inom Skatteverket har rätt till direktåtkomst i beskattningsdatabasen införts utan att det utifrån förarbetena har varit möjligt att göra en avvägning mellan behovet av en sådan åtkomst och dess effektivitet å ena sidan och konsekvenserna för integritetsskyddet å andra sidan.

6 Exekutionsväsendet

Huvudsaklig bedömning:

– En förstärkt sekretess infördes i Kronofogdemyndighetens verksamhet i syfte att möjliggöra ett ökat uppgiftsutbyte med andra myndigheter utan att en tillräcklig redovisning lämnades av de från integritetssynpunkt relevanta effekterna. De nödvändiga avvägningarna mellan effektivitets- och integritetsintressen har därför inte varit möjliga att göra.
– Bestämmelser om behandling av personuppgifter, som tar sikte på eller får återverkan på frågan om utlämnande av uppgifter från Kronofogdemyndigheten, har utformats utan att det tydliggjorts hur bestämmelserna förhåller sig till regler om sekretess.
– Den införda sekretessen i Kronofogdemyndighetens verksamhet för enstaka betalningsförsummelser har inneburit en förstärkning av integritetsskyddet. Bestämmelserna om rättelse i personuppgiftslagen tolkas dock olika hos skilda verksamhetsgrenar inom Kronofogdemyndigheten. Även uppgifter som myndigheten själv uppfattar som missvisande lämnas därför alltjämt ut till kreditupplysningsföretag.

6.1 Allmänt om exekutionsväsendet

Den 1 juli 2006 avvecklades de tio regionala kronofogdemyndigheterna och en ny myndighet med rikstäckande verksamhet, benämnd Kronofogdemyndigheten, inrättades (prop. 2005/06:200, bet. 2005/06:SkU35). Denna myndighet är knuten till Skatteverket i strategiska frågor och för utnyttjande av gemensamt stöd när det gäller IT-verksamheten och administrativa stödfunktioner. I lagstiftningsärendet slogs också fast att ansvaret för behandling av

personuppgifter i Kronofogdemyndighetens verksamhet odelat skall ligga på Kronofogdemyndigheten.

Kronofogdemyndigheten ansvarar för indrivning av statliga fordringar, dvs. skatter och avgifter, men även för verkställighet av enskildas betalningsanspråk. Myndigheten har också till uppgift att svara för bl.a. frågor om frivillig skuldsanering och om tillsyn i och lönegaranti vid konkurs. Som huvudregel är det Skatteverket som företräder staten i domstol inom exekutionsväsendets verksamhetsområde.

6.2 Kort om regelverket

6.2.1 Sekretess i exekutionsväsendet

Exekution

Inom den nya rikstäckande myndigheten Kronofogdemyndigheten kommer verksamhetsgrenar att uppträda självständigt i förhållande till varandra (prop. 2005/06:200 s. 146 f.). Inrättandet av den nya myndigheten har därför inte ansetts innebära några förändrade sekretessgränser inom denna myndighet.

I 9 kap. 19 § SekrL ges föreskrifter om sekretess inom Kronofogdemyndighetens exekutiva verksamhet för uppgift om enskildas personliga eller ekonomiska förhållanden. Enligt första stycket gäller sekretess i mål eller ärende angående utsökning och indrivning, dvs. vid all tillämpning av utsökningsbalken och andra verkställighetsregler. Även Kronofogdemyndighetens uppgift att företräda staten i allmänna mål enligt lagen (1993:891) om indrivning av statliga fordringar samt verksamhet enligt 21 § (1994:466) om särskilda åtgärder i beskattningsförfarandet omfattas av denna sekretess, liksom verksamhet enligt lagen (1986:436) om näringsförbud, eftersom det i denna sistnämnda verksamhet ofta förekommer integritetskänsliga uppgifter rörande t.ex. hälsa och brottsmisstankar.

I Kronofogdemyndighetens uppgifter ingår numera inte enbart att göra en undersökning av gäldenärens tillgångar. En gäldenärsutredning skall också göras. I denna undersöks den totala skuldsättningen, orsaken till skuldernas uppkomst, näringsverksamhets omsättning och resultat och möjligheter till återvinning. Dessutom görs en prognos avseende gäldenärens betalningsförmåga. I en gäldenärsutredning kan alltså ingå både uppgifter från

deklarationshandlingar och mer ömtåliga uppgifter om exempelvis anstaltsvistelser, arbetslöshet och sjukdomar.

Sekretess i Kronofogdemyndighetens verksamhet gällde tidigare med ett rakt skaderekvisit, dvs. presumtionen var för offentlighet. Genom lagstiftning som trädde i kraft den 1 oktober 2001 gäller sekretessen numera med omvänt skaderekvisit.

I samband med att den förstärkta sekretessen infördes i Kronofogdemyndighetens verksamhet har regeringen i den vid samma tillfälle införda förordningen (2001:590) om behandling av uppgifter i Kronofogdemyndighetens verksamhet infört bestämmelser om viss uppgiftsskyldighet för kronofogdemyndigheterna i förhållande till Tullverket, Skatteverket och Säkerhetspolisen. Någon sådan uppgiftsskyldighet synes inte tidigare ha varit föreskriven (jfr utsökningsregisterlagen [1986:617] och utsökningsregisterförordningen [1986:678]).

För vissa uppgifter gäller undantag från sekretessen enligt 9 kap. 19 § SekrL. Så är fallet för uppgift om förpliktelse som avses med sökt verkställighet i ett pågående mål. Ett mål är pågående från det att det kommit in till kronofogdemyndigheten till dess att det är klart och redovisas tillbaka till sökanden.

Enligt 9 kap. 19 § andra stycket SekrL gäller sekretess inte beslut i ett mål eller ärende. Skälet är det starka insynsintresse som föreligger i ärenden inom exekutionsväsendet och där beslut kan avse ingripande åtgärder för den enskilde, t.ex. i form av utmätning, avhysning och handräckning.

Motsvarande sekretess som enligt första stycket, dvs. med ett omvänt skaderekvisit, gäller enligt 9 kap. 19 § SekrL tredje stycket också i myndighets verksamhet som avser förande av eller uttag ur utsöknings- och indrivningdatabasen enligt lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet för uppgift som har tillförts databasen. Enligt 26 och 27 §§ nämnda lag får Skatteverket, Tullverket och Säkerhetspolisen ha direktåtkomst till utsöknings- och indrivningsdatabasen.

Eftersom en konkursförvaltare inte är en myndighet eller ett därmed jämställt organ är bestämmelserna om uppgiftsutbyte i bl.a. 14 kap. 1 och 3 §§ SekrL inte tillämpliga hos denne. I 9 kap. 19 § fjärde stycket föreskrivs därför att uppgifter får lämnas till konkursförvaltare utan hinder av sekretessen inom exekutionsväsendet.

Skuldsanering

Enligt 7 kap. 35 § SekrL gäller sekretess hos Kronofogdemyndigheten i ärende om skuldsanering för uppgift om enskilds personliga förhållanden, om det kan antas att den enskilde eller någon honom närstående lider men om uppgiften röjs. Sekretess gäller således med ett rakt skaderekvisit, dvs. med presumtion för offentlighet. Skuldsanering kan enligt skuldsaneringslagen (1994:334) ske antingen frivilligt efter fastställelse av Kronofogdemyndigheten eller i tvingande form efter beslut av allmän domstol.

I 37 § skuldsaneringslagen föreskrivs att socialnämnder och andra myndigheter skall överlämna sådana uppgifter om en gäldenärs personliga och ekonomiska förhållanden som behövs för prövning av ett skuldsaneringsärende till Kronofogdemyndigheten och domstolar som handlägger ärenden om skuldsanering. Detta innebär en sekretessbrytande uppgiftsskyldighet som tar över den sekretess som hos socialnämnden gäller för uppgifterna enligt 7 kap. 4 § SekrL (jfr 14 kap. 1 §). Uppgiftsskyldigheten omfattar dock inte uppgifter om närstående till gäldenären.

Sekretessen enligt 7 kap. 35 § SekrL gäller också hos domstol och hos kommunal konsumentvägledare. Själva besluten i ett skuldsaneringsärende omfattas emellertid inte av någon sekretess.

En mer utförlig redovisning av sekretessbestämmelserna i Kronofogdemyndighetens verksamhet lämnas i kapitel 25.

6.2.2 Behandling av personuppgifter

Vid den tidigare omtalade reformen beträffande behandling av personuppgifter inom skatt, tull och exekution kom lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet att ersätta utsökningsregisterlagen (1986:617), lagen (1991:876) om register för betalningsföreläggande och handräckning samt förordningen (1994:348) om register för skuldsaneringsärenden. Kronofogdemyndigheten hade också tillstånd att föra vissa andra register enligt föreskrifter i förordning eller enligt tillstånd från Datainspektionen, vilka också upphörde att gälla i samband med reformen och ersattes av den nya lagen.

Lagen om behandling av uppgifter i Kronofogdemyndighetens verksamhet innehåller i 1 kap. vissa gemensamma bestämmelser som rör behandling av personuppgifter utanför myndighetens

databaser. Databaserna – som utgörs av utsöknings- och indrivningsdatabasen, betalnings- och handräckningsdatabasen, skuldsaneringsdatabasen samt konkurstillsynsdatabasen – regleras i 2 kap. De olika databaserna har där reglerats särskilt i fråga om ändamål, vilka uppgifter som får behandlas samt gallring. Därutöver finns gemensamma bestämmelser om bl.a. direktåtkomst och sökbegrepp.

En mer utförlig redovisning av bestämmelserna i lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet lämnas i kapitel 25.

6.2.3 Kronofogdemyndighetens rätt att använda vissa tvångsmedel

Utsökningsbalken (UB) är enligt dess 1 kap. 1 § tillämplig i fråga om verkställighet av dom eller annan exekutionstitel, som innefattar betalningsskyldighet eller annan förpliktelse, samt i fråga om verkställighet av beslut om kvarstad eller annan liknande säkerhetsåtgärd.

I 1 kap. 3 § UB föreskrivs att verkställighet åvilar Kronofogdemyndigheten.

Förfarandet hos Kronofogdemyndigheten regleras i 2 kap. UB. I 2 kap. 15–17 §§ finns bestämmelser om myndighetens rätt att använda tvångsmedel.

Av 2 kap. 17 § UB framgår att Kronofogdemyndigheten under vissa förutsättningar har rätt till intrång. Ytterligare bestämmelser rörande Kronofogdemyndighetens rätt till intrång finns i utsökningsförordningen (1981:981).

En mer utförlig redovisning av reglerna om Kronofogdemyndighetens rätt att använda vissa tvångsmedel lämnas i kapitel 25.

6.3 Sammanfattning och bedömning

6.3.1 Förstärkt sekretess inom Kronofogdemyndigheten

I samband med den lagstiftningsreform som under år 2001 genomfördes rörande bl.a. Skatteverkets och Kronofogdemyndighetens behandling av personuppgifter förstärktes också sekretessen på de dåvarande kronofogdemyndigheternas område. Man ville på så sätt dels komma till rätta med svårigheter vid informations-

utbyte med andra myndigheter, dels tillförsäkra de enskilda som är föremål för kronofogdemyndigheternas åtgärder ett starkare sekretesskydd. När det gällde det förstnämnda skälet syftade det alltså till att öka effektiviteten i andra myndigheters informationsutbyte med kronofogdemyndigheterna. Om sekretessen förstärktes, skulle de utlämnande myndigheterna få större möjlighet att lämna uppgifter till kronofogdemyndigheterna.

I fråga om uppgiftsutbyte mellan myndigheter gäller enligt 14 kap. 1 § SekrL att sekretess inte hindrar att uppgift lämnas till annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Bestämmelser om att en myndighet *får* lämna ut uppgifter till en annan har däremot inte den verkan att sekretessen viker på motsvarande sätt (Regner, s. 14:10).

Innebörden av 14 kap. 1 § SekrL är att det inte spelar någon roll med vilka styrka sekretess gäller, dvs. om det är fråga om ett rakt eller omvänt skaderekvisit eller om sekretessen är absolut. Sekretessen viker nämligen alltid för den i lag eller förordning föreskrivna uppgiftsskyldigheten. Ett uppgiftsutbyte som sker på grund av en sådan föreskriven uppgiftsskyldighet påverkas alltså inte av att sekretessen stärks eller försvagas. Av intresse i lagstiftningsärendet om förstärkt sekretess i kronofogdemyndigheternas verksamhet hade därför varit att få en redovisning av vilket uppgiftsutlämnande som sker till Kronofogdemyndigheten enligt 14 kap. 1 § på grund av uppgiftsskyldighet hos andra myndigheter. Därigenom skulle man ha erhållit en mer fullständig bild av vilket uppgiftsutlämnande som i övrigt skulle ske med stöd av 14 kap. 3 § och som den förstärkta sekretessen avsåg att underlätta. Om uppgiftsutlämnandet enligt 14 kap. 3 § på detta sätt hade varit närmare definierat hade det varit lättare att bedöma behovet av att effektivisera just detta uppgiftsutlämnande och att väga detta behov mot enskildas intresse av skydd för sina uppgifter. Någon redovisning av i vilken utsträckning andra myndigheter hade och avsågs ha en föreskriven uppgiftsskyldighet i förhållande till kronofogdemyndigheterna lämnades dock inte i lagstiftningsärendet. I vart fall Skatteverket har en föreskriven uppgiftsskyldighet i förhållande till Kronofogdemyndigheten, som torde täcka myndighetens primära behov av uppgifter från beskattningsverksamheten. I vilken utsträckning andra myndigheter också har uppgiftsskyldighet i förhållande till Kronofogdemyndigheten är svårt att närmare bedöma.

Sammanfattningsvis bör understrykas att en noggrann redovisning av de från integritetssynpunkt relevanta effekterna är önsk-

värd i lagstiftningsärenden som i likhet med det här redovisade ärendet får betydelse för den personliga integriteten. I annat fall blir det i praktiken inte möjligt att göra de erforderliga avvägningarna mellan effektivitets- och integritetsintressen.

6.3.2 Behandling av personuppgifter

Bestämmelserna som reglerar behandling av personuppgifter inom Kronofogdemyndighetens verksamhet kom till inom ramen för en reform år 2001 som också omfattade Skatteverket och Tullverket, och reglerna kom att utformas på samma sätt. Den kritik som ovan lämnats i fråga om registerlagstiftningen på Skatteverkets område – att bestämmelser om behandling av personuppgifter, som tar sikte på eller får återverkan på frågan om utlämnande av uppgifter från den aktuella verksamhet, har utformats utan att det tydliggjorts hur bestämmelserna förhåller sig till regler om sekretess – träffar därför också reglerna om behandling av personuppgifter hos Kronofogdemyndigheten.

6.3.3 Rättelse av uppgifter i Kronofogdemyndighetens databaser

Datainspektionen genomförande har under oktober–december 2002 ett antal inspektioner hos åtta myndigheter som behandlar personuppgifter som registreras i Kronofogdemyndighetens exekutiva verksamhet och hos kreditupplysningsföretag som utnyttjar sådana uppgifter. Två av myndigheterna var kronofogdemyndigheter. Därutöver undersökte Datainspektionen effekterna av den ändrade sekretesslagstiftningen inom exekutionsväsendet och möjligheten att bedöma enstaka betalningsförsummelsers relevans för kreditupplysningsföretagens kreditupplysningsverksamt samt de tänkbara effekterna om en beloppsgräns införs.

I en rapport den 25 februari 2004 redovisade Datainspektionen resultatet av inspektionerna och av observerade effekter av den nya sekretessregleringen. Därvid konstaterade inspektionen att bestämmelserna i personuppgiftslagen om rättelse hade tolkats olika hos kronofogdemyndigheterna. Såvitt kunde bedömas varierade även domstolarnas praxis i denna fråga. En av de inspekterade kronofogdemyndigheterna, Kronofogdemyndigheten i Stockholm, ansåg

att förutsättningarna för att rätta i utsökningsregistret förändrats när personuppgiftslagen ersatte datalagen. Denna kronofogdemyndighet rättade inte längre uppgifter som visserligen var missvisande, men inte felaktiga, i förhållande till registrets ändamål. En konsekvens av denna tolkning var att uppgifter som var missvisande kom att lämnas ut till kreditupplysningsföretag och registreras i kreditupplysningsregister, trots att de där såsom missvisande uppgifter enligt kreditupplysningslagen inte fick förekomma.

Datainspektionen gör bedömningen att förutsättningarna för rättelse i utsökningsregistret inte ändrats genom att datalagen ersatts med personuppgiftslagen. Inspektionen anser att bestämmelserna om rättelse i personuppgiftslagen (28 §) innebär att uppgifter som är objektivt sett missvisande i förhållande till ändamålet med behandlingen också är att anse som felaktiga i personuppgiftslagens mening och därför skall rättas.

Beträffande de nya sekretessreglerna hos kronofogdemyndigheterna konstaterar Datainspektionen att dessa lett till att många gäldenärer har undgått betalningsanmärkning genom att till kronofogdemyndigheten snabbt betala sin skuld. De nya reglerna torde också ha bidragit till att antalet framställningar om rättelse i utsökningsregistret hade halverats sedan år 2000.

Det hade vid inspektioner framkommit att det finns flera sorters beslut och andra åtgärder från kronofogdemyndigheternas sida, t.ex. beslut om avbetalningsplan och vidtagna indrivningsåtgärder, som leder till att sekretesskyddet för enstaka uppgifter om s.k. restföring inte får avsedd effekt. Därutöver hade framkommit att det finns sätt att kringgå den nya sekretessbestämmelsen, bland annat var det möjligt att genom muntlig förfrågan om viss gäldenär indirekt få uppgift om eventuell restförd skuld. Inspektionen framhåller att om detta utnyttjas av kreditgivare kommer lagstiftningens syfte att motverkas.

Datainspektionens kritik synes i allt väsentligt ha fog för sig. Från integritetsskyddssynpunkt kan det inte anses tillfredsställande att bestämmelserna om rättelse i personuppgiftslagen tolkas olika inom olika verksamhetsgrenar och att även uppgifter som Kronofogdemyndigheten själv uppfattar som missvisande alltjämt lämnas ut till kreditupplysningsföretag.

7 Kreditupplysning och inkasso

Huvudsaklig bedömning:

– Det är inte tillfredsställande att skyddet för den enskildes integritet, som annars följer av framför allt kreditupplysningslagen, inte kan upprätthållas vid kreditupplysning via Internet eller andra elektroniska kommunikationstjänster.
– Regelverket på området för inkasso föranleder inte några särskilda anmärkningar från integritetsskyddssynpunkt.

7.1 Allmänt om kreditupplysning och inkasso

7.1.1 Kreditupplysning

I syfte att förenkla och för att minska kostnaderna för utlåning och kreditgivning anlitar banker och andra kreditgivare särskilda kreditupplysningsföretag som har till affärsidé att tillhandahålla information om den som söker kredit eller lån. För att bedriva kreditupplysningsverksamhet krävs tillstånd av Datainspektionen. Det finns för närvarande 17 företag som har sådant tillstånd. Av dessa har sex företag rikstäckande register som omfattar samtliga svenskar över 15 år oavsett om de har någon betalningsanmärkning eller inte. Kreditupplysningsverksamhet skall bedrivas enligt reglerna i kreditupplysningslagen (1973:1173).

7.1.2 Inkasso

Ett kreditupplysningsverksamheten närliggande område som också har ansetts medföra behov av en särskild skyddsreglering är inkassoverksamhet. Sådan verksamhet regleras i inkassolagen (1974:182). Inkassoverksamhet kan bedrivas antingen som egen-

inkasso (när en fordringsägare som själv driver näringsverksamhet driver in fordringar som uppkommit i den egna verksamheten) eller som genom ombud bedriven inkassoverksamhet. För det sistnämnda krävs tillstånd av Datainspektionen, dock inte om verksamheten bedrivs av företag under Finansinspektionens tillsyn eller av advokater. Det är för närvarande ett par hundra företag som har Datainspektionens tillstånd att bedriva inkassoverksamhet.

7.2 Kort om regelverket

7.2.1 Kreditupplysningslagen

Kreditupplysningslagen syftar i första hand till att undanröja riskerna för att kreditupplysning skall medföra otillbörligt intrång i de kreditsökandes personliga integritet eller leda till skada genom oriktiga eller missvisande uppgifter. Samtidigt är lagen avsedd att bidra till en effektivt fungerande kreditupplysningsverksamhet. Numera lämnas kreditupplysningar dock i stor utsträckning med hjälp av andra medier än som tidigare var fallet, medier som omfattas av grundlagsskydd enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Skyddsreglerna i kreditupplysningslagen, t.ex. i fråga om krav på legitimt behov hos den som begär kreditupplysning och om skyldighet att lämna information till den som upplysningen avser, gäller därmed inte när den typen av medier används. I augusti 2003 påbörjades därför en översyn av kreditupplysningslagen inom Justitiedepartementet. En huvudfråga för denna översyn var om kreditupplysningslagen behöver ändras för att skyddet för den enskildes integritet alltjämt skall vara tillfredsställande. Översynen har ännu inte avslutats.

7.2.2 Inkassolagen

Inkassolagen syftar i första hand till att skydda gäldenärer – såväl fysiska som juridiska personer – mot otillbörliga inkassometoder, t.ex. i form av trakasserier eller onödiga kostnader, och därav uppkommande skador och olägenheter. Datainspektionen har tillsyn över att inkassolagens bestämmelser följs och att inkassoverksamhet därvid bedrivs enligt god inkassosed. Som inkassoåtgärder räknas krav eller andra påtryckningar mot en gäldenär för att förmå

denne att betala sin skuld. Rena betalningspåminnelser räknas dock inte som inkassoåtgärder.

En mer utförlig redovisning av gällande regler på områdena för kreditupplysning och inkasso lämnas i kapitel 26.

7.3 Sammanfattning och bedömning

7.3.1 Kreditupplysning via nya medier

Kreditupplysningar lämnas idag via bl.a. Internet, vilket aktualiserar frågan om ett offentliggörande på detta sätt skyddas av reglerna i tryckfrihetsförordningen (TF) och yttrandefrihetsgrundlagen (YGL).

Regeringsrätten har i RÅ 2003 ref. 30 prövat frågan om ett kreditupplysningsföretag genom tillhandahållande av en webbtjänst omfattades av grundlagsskyddet i 1 kap. 9 § YGL, den s.k. databasregeln. Genom webbtjänsten hade abonnenter tillgång till de uppgifter som publicerats i en periodisk skrift som företaget utgivit. Datainspektionen hade ansett att företaget inte omfattades av databasregeln, eftersom det inte var ett traditionellt massmedieföretag och inte hade en sådan redaktion som avses i denna regel. Regeringsrätten fann att de personer som för företagets räkning redigerade den periodiska skriften tillsammans bildade en redaktion i yttrandefrihetsgrundlagens mening. Då det inte heller i övrigt framkommit några hinder för tillämpning av databasregeln kunde kreditupplysningslagens bestämmelser om krav på legitimt behov och kreditupplysningskopia inte göras gällande beträffande den verksamhet som bedrevs av företaget.

Genom ändringar i yttrandefrihetsgrundlagen, som trädde i kraft den 1 januari 2003, kan vem som helst som yttrar sig via Internet få grundlagsskydd, under förutsättning att en ansvarig utgivare utses och att ansökan om ett s.k. frivilligt utgivarbevis sker och beviljas (se kapitel 23).

Om kreditupplysningar lämnas i form av offentliggöranden på sätt som avses i tryckfrihetsförordningen och yttrandefrihetsgrundlagen gäller, som berörts tidigare, vissa undantag från reglerna i kreditupplysningslagen. Sålunda gäller inte kravet på att den som bedriver kreditupplysningsverksamhet skall ha *tillstånd* av Datainspektionen. Undantag görs också från bestämmelsen om att kreditupplysningar om privatpersoner inte får lämnas ut, om det

finns anledning att anta att upplysningar kommer att användas av någon annan än den som på grund av ett ingånget eller ifrågasatt kreditavtal eller av någon annan liknande anledning har behov av upplysningen (*kravet på legitimt behov*). Inte heller kravet på att lämna *kreditupplysningskopia* med beställaruppgift till den som avses med upplysningen gäller när kreditupplysningen offentliggörs på sådant sätt som avses i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Skyldigheten att *rätta* en oriktig eller missvisande uppgift i en kreditupplysning som lämnas genom offentliggörande på detta sätt är begränsad och gäller endast beträffande periodisk skrift samt kreditupplysningsverksamhet som bedrivs genom återkommande offentliggöranden enligt yttrandefrihetsgrundlagen.

I augusti 2003 påbörjades en översyn av kreditupplysningslagen inom Justitiedepartementet. Förutom huvudfrågan om kreditupplysningslagen – mot bakgrund av att kreditupplysning numera lämnas med hjälp av andra medier än som tidigare var fallet – behöver ändras för att skyddet av den enskildes integritet alltjämt skall vara tillfredsställande, skulle det också övervägas om en generell reglering av förhållandet mellan reglerna i kreditupplysningslagen och reglerna i tryckfrihetsförordningen och yttrandefrihetsgrundlagen bör införas. Vid översynen skulle också övervägas om skyddet för den enskilde behöver stärkas när det bara handlar om enstaka betalningsförsummelser. Vissa andra frågor om kreditupplysningar skulle också ses över.

Enligt uppdragsbeskrivningen för översynen ingick i denna att göra en analys av vilka risker från integritetssynpunkt som de nya teknikerna innebär vid kreditupplysning och hur dessa risker kan minskas. Översynen fick dock inte utmynna i förslag till grundlagsändringar, utan skulle ta sikte på vilka skärpningar av regelsystemet som är möjliga att åstadkomma på annat sätt.

Översynen har ännu inte avslutats och än mindre lett fram till något förslag om lagändringar. I sin årsredovisning för 2005 angav Datainspektionen att det hade kommit in många klagomål avseende nya kreditupplysningstjänster som erbjuds via SMS och en webbplats.

Från ett integritetsskyddsperspektiv kan det inte anses tillfredsställande att det skydd mot otillbörliga intrång i de kreditsökandes personliga integritet, i form av t.ex. legitimt behov och kreditupplysningskopia, eller mot skada genom oriktiga eller missvisande uppgifter som kreditupplysningslagen avser att ge, inte kan upp-

rätthållas då kreditupplysningar ges via Internet eller andra elektroniska kommunikationstjänster.

7.3.2 Enstaka betalningsförsummelser

Den förstärkning av sekretessen på exekutionsområdet (9 kap. 19 § SekrL) som infördes år 2001, och som bl.a. innebar att sekretess numera gäller i avslutade mål som avser en enstaka betalningsförsummelse, innebar även en viss förstärkning av integritetsskyddet för enskilda. I samband med att lagförslaget behandlades i riksdagen anförde finansutskottet i sitt av riksdagen godkända betänkande 2000/01:FiU21 att regeringen borde överväga andra metoder för att förhindra kreditupplysningsföretagen att i kreditupplysningar lämna information om enstaka mindre betalningsförsummelser, om det skulle visa sig att de skärpta sekretessreglerna inte var tillräckliga för att komma till rätta med de problem som är förknippade med sådana uppgifter. Utskottet ansåg att det i fråga om fysiska personer fanns anledning att överväga att införa en beloppsgräns för vilka skulder som får finnas med i en kreditupplysning. Som alternativa metoder nämnde utskottet en gräns knuten till antalet mindre betalningsförsummelser eller en kortare gallringstid för mindre betalningsförsummelser. Vad utskottet anfört borde ges regeringen till känna.

Enligt den tidigare nämnda uppdragsbeskrivningen för Justitiedepartementets översyn av kreditupplysningslagen skulle också de konsekvenser som de ändrade sekretessreglerna för utsöknings- och indrivningsverksamheten har fått för kreditupplysningsverksamheten och för enskilda utvärderas. På grundval av den gjorda utvärderingen skulle övervägas om de genomförda lagändringarna är tillräckliga eller om ytterligare åtgärder behöver vidtas för att undvika att enstaka mindre betalningsförsummelser får orimliga följder för den enskilde. En avvägning skulle då göras mellan, å ena sidan, intresset av en effektiv kreditupplysningsverksamhet och av att kreditupplysningar är så lättillgängliga och fullständiga som möjligt och, å andra sidan, hänsynen till den personliga integriteten och enskildas intresse av att missförstånd eller enstaka ekonomiska försummelser inte orimligt begränsar deras ekonomiska handlingsutrymme. Inte heller denna del av Justitiedepartementets översyn av kreditupplysningslagen är avslutad.

7.3.3 Reglerna för inkasso fungerar tillfredsställande

Såvitt kartläggningen har kunnat utvisa fungerar skyddet för den enskildes personliga integritet, såsom det reglerats i inkassolagen samt i personuppgiftslagen, tillfredsställande på området för inkasso. Av tillsynsmyndighetens – Datainspektionens – redovisning framgår visserligen att den tillsyn som bedrivs på området har föranlett kritik i knappt hälften av fallen (år 2005) samt att klagomål förekommer. De brister som på detta sätt har framkommit förefaller dock inte ha sin grund i att regelverket skulle vara på något sätt bristfälligt från integritetsskyddssynpunkt.

8 Domstolarna

Huvudsaklig bedömning:

– Reglerna på domstolsområdet, som i många fall ger intresset av offentlig insyn företräde framför enskildas intresse av skydd för den personliga integriteten, är tydliga och grundade på sedan lång tid vedertagna värderingar.
– Mot bakgrund av flera JO- och JK-beslut rörande handläggning av sekretessfrågor kan det sättas i fråga om inte mer resurser bör läggas på domstolarnas handläggning av sådana frågor, framför allt i form av utbildning.
– Det är inte tillfredsställande att domstolarnas behandling av personuppgifter ännu inte har blivit föremål för någon lagreglering.

8.1 Allmänt om domstolarna

Till allmänna domstolar räknas tingsrätterna, hovrätterna och Högsta domstolen. Dessa domstolars huvuduppgift är att avgöra tvistemål och brottmål. Dessutom utövar de en viss offentlig kontroll, bl.a. genom att ge tillstånd till adoptioner och vissa namnbyten. Några av tingsrätterna har också särskilda domstolsfunktioner. Dit hör handläggning av miljömål, fastighetsmål, sjörättsliga mål och tryckfrihetsmål.

De allmänna förvaltningsdomstolarna utgörs av länsrätterna, kammarrätterna och Regeringsrätten. Förvaltningsdomstolarnas främsta uppgift är att lösa tvister mellan den enskilde och det allmänna i form av kommun, landsting och stat. Vid dessa domstolar handläggs t.ex. beslut om tvångsingripanden för ungdoms-, missbruks- eller psykiatrivård, skattemål och socialförsäkringsmål. Andra exempel är mål enligt plan- och bygglagen och social-

bidragsmål. Utlännings- och medborgarskapsmål prövas sedan den 1 april 2006 av länsrätterna i Stockholm, Göteborg och Malmö samt av Kammarrätten i Stockholm.

Vid sidan av allmänna domstolar och allmänna förvaltningsdomstolar finns ett fåtal specialdomstolar, framför allt Arbetsdomstolen och Marknadsdomstolen. Dessa avgör tvister inom olika specialområden där det har ansetts kräva särskild sakkunskap.

Utvecklingen inom domstolsväsendet har på senare tid gått mot en större renodling av verksamheten till förmån för dömande uppgifter. Alltjämt handlägger domstolarna emellertid en rad ärendefrågor samt utövar förliknings- och medlingsverksamhet. Till följd av verksamhetens karaktär förekommer uppgifter om enskilds personliga förhållanden i stor omfattning. Uppgifterna är många gånger av känslig natur. I vissa fall är det den enskilde som själv väcker talan vid en domstol och därvid, som grund för sin talan, bifogar uppgifter om sina personliga förhållanden. I andra fall lämnas uppgifterna till domstolen från en motpart, som antingen själv har tagit initiativ till den rättsliga processen eller svarar på den enskildes talan i målet eller ärendet. Motparten utgörs många gånger av en myndighet.

8.2 Kort om regelverket

Det är en grundläggande princip att den dömande verksamheten skall ske under stor öppenhet. Regler för t.ex. partsinsyn, bevisföring och för offentliggörande av domar och andra beslut kan därmed innebära att uppgifter om enskilds personliga förhållanden, som i andra sammanhang är skyddade, blir tillgängliga för utomstående.

Eftersom det hos domstolarna inom ramen för deras rättskipande och rättsvårdande verksamhet förekommer en mängd uppgifter om enskilds personliga förhållanden har det dock ansetts nödvändigt med regler som syftar till att skydda sådana uppgifter. Sådana regler finns framför allt i 12 kap. SekrL. Där föreskrivs vilken sekretess som gäller om domstol hållit förhandling inom stängda dörrar, vilken inverkan en förhandling inför domstolen har på sekretesskyddet och när det är möjligt att sekretessbelägga uppgifter i domar och beslut. I sekretesslagen finns också vissa särskilda bestämmelser om sekretess hos domstolarna. Som exempel kan nämnas 7 kap. 22 § SekrL om sekretess i brottmål för uppgift

om enskilds personliga förhållanden som kommer fram vid en särskild personutredning, rättpsykiatrisk utredning eller annan sådan utredning. Andra exempel är 9 kap. 15 och 16 §§, där behovet av skydd för parter, målsägande eller andra inblandade har ansetts så starkt i vissa typer av mål att offentligheten har fått vika.

I rättegångsbalken och förvaltningsprocesslagen finns regler om domstols möjlighet att få tillgång till bevis som innebär att den sekretess eller tystnadsplikt för uppgift om enskilds personliga förhållanden, som annars gäller, i vissa fall skall brytas inom ramen för den rättsliga processen. Bestämmelserna om partsinsyn, vittnesförhör, editionsplikt och om sakkunnig kan innebära en sådan sekretessbrytande uppgiftsskyldighet i domstolen. Omständigheterna i målet kan emellertid vara sådana att rätten har möjlighet att förordna att förhandling skall hållas inom stängda dörrar.

Sekretessregleringen har utformats med särskild hänsyn till de speciella förhållandena som hör samman med dömande verksamhet. Detta, och den omständigheten att det hos domstolarna kan förekomma mål och ärenden av mycket skiftande slag, har medfört att regleringen blivit förhållandevis komplicerad.

Beträffande behandling av personuppgifter hos domstolarna gäller förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling, förordningen (2001:640) om registerföring m.m. vid länsrätt med hjälp av automatiserad behandling och förordningen (2001:641) om registerföring m.m. vid Regeringsrätten och kammarrätterna med hjälp av automatiserad behandling.

Vad som sagts ovan om offentlighet och sekretess vid domstol gäller i allt väsentligt också Arbetsdomstolen och Marknadsdomstolen (jfr 5 kap. 3 § lagen [1974:371 om rättegången i arbetstvister och 16 § lagen [1970:417] om marknadsdomstol). De särskilda författningarna rörande behandling av personuppgifter på domstolsområdet omfattar däremot inte Arbetsdomstolen och Marknadsdomstolen.

En mer utförlig redogörelse för regler som berör skyddet för den enskildes integritet på domstolsområdet lämnas i kapitel 27.

8.3 Sammanfattning och bedömning

8.3.1 Gällande regler

Sammanfattande kommentar rörande regelverket

Från rättssäkerhetssynpunkt har det sedan lång tid tillbaka ansetts vara av vikt att domstolarnas handläggning och beslut i så stor utsträckning som möjlighet sker under öppenhet. Att den rättskipande och rättsvårdande verksamheten är underkastad offentlig insyn har också ansetts betydelsefullt för allmänhetens förtroende för rättskipningen. I grundlagen har det slagits fast att förhandling vid domstol som huvudregel skall vara offentlig (2 kap. 11 § andra stycket RF).

Med hänsyn till att det i domstolarnas dömande verksamhet förekommer en mängd uppgifter om enskilds personliga förhållanden av mer eller mindre känslig natur har det dock ansetts ofrånkomligt att begränsa den offentliga insynen genom sekretessregler. Sekretess kan gälla hos domstolen antingen genom primär sekretess som gäller direkt hos domstolen, eller genom sekundär sekretess som överförs till domstolen från domstol eller annan myndighet. Sekretess kan även komma att gälla för uppgifter om enskild under endast en del av en domstols handläggning av ett mål, eftersom reglerna föreskriver att domstolen vid flera tillfällen – t.ex. när det gäller frågan om förhandling skall hållas inom stängda dörrar eller om sekretess skall gälla för uppgifter som tas in i en dom – skall ta ställning till om sekretessen skall bestå eller inte. Offentlighetsintresset har ansetts väga särskilt tungt i de allmänna domstolarna. För att frångå principer om öppenhet vid förhandling i allmän domstol krävs inte endast att sekretess gäller för uppgifter som kan förebringas vid förhandlingen, utan det skall också bedömas som synnerligen viktigt att uppgiften i fråga hålls hemlig.

Sekretessregleringen på domstolsområdet är sådan att det med något undantag har överlämnats åt domstolen själv att i samband med olika åtgärder under handläggningen av ett mål avgöra huruvida offentlighets- eller sekretessintressen skall tilläggas störst tyngd. Domstolarna har således ålagts ett stort eget ansvar att se till att erforderliga avvägningar görs och att därvid artikel 8 i Europakonventionen om den enskildes rätt till respekt för sitt privatliv iakttas. Beslut att förordna om stängda dörrar eller om sekretess kan överklagas i den ordning som gäller för respektive domstol. Ett

beslut av en domstol som innebär att uppgifter *inte* skall hemlighållas, kan däremot inte överklagas.

Den omständigheten att det i stor utsträckning har överlämnats till domstolen själv att avgöra huruvida offentlighets- eller sekretesshänsyn skall väga tyngst i samband med olika handläggningsåtgärder innebär att det ställs särskilda krav på domarnas utbildning i dessa frågor och att det finns möjlighet, om inte annat i form av tid, att ta ställning till dessa ofta relativt komplicerade frågor. Domstolarnas tillämpning av sekretessreglerna på domstolsområdet har emellertid föranlett ett flertal beslut av såväl JK som JO där felaktigheter i handläggningen har konstaterats (se t.ex. JK i ett beslut 2003-03-28, dnr 606-03-22, där kritiska synpunkter framfördes mot en tingsrätt för omfattningen av ett sekretessförordnande i en brottmålsdom, samt JO 1986/87 s. 28, där kritik riktades mot en tingsrätt för att den inte tillräckligt omsorgsfullt hade berett frågan huruvida en rättspsykiatrisk undersökning skulle föredras inom stängda dörrar).

När det gäller regelverket för *behandling av personuppgifter* kan det konstateras att samtliga domstolar numera använder sig av datorteknik för att framställa domar, beslut och andra dokument. Domstolarna har också tillgång till större datorsystem som ett stöd i verksamheten.

Fram till år 2001 fanns inte någon enhetlig reglering av domstolarnas behandling av personuppgifter. Regleringen återfanns i stället i olika förordningar eller i tillstånd meddelade av Datainspektionen. Det förekom även behandling av personuppgifter som inte omfattades av någon särskild reglering. Den reglering som fanns avsåg – i enlighet med då gällande generella regler i datalagen – endast behandling av personuppgifter i personregister. Behandling av personuppgifter i löpande text var således helt oreglerad.

Något förslag till en ny reglering av behandling av personuppgifter på domstolsområdet hade inte arbetats fram innan personuppgiftslagen trädde i kraft den 24 oktober 1998. I stället fick Domstolsdatautredningen i uppdrag att ta fram ett förslag på en reglering, som var anpassad till EG:s dataskyddsdirektiv och personuppgiftslagen, inför det att övergångsbestämmelserna till datalagen skulle upphöra att gälla den 1 oktober 2001. Domstolsdatautredningen lämnade förslag till tre förordningar på domstolsområdet, som närmast fick betraktas som en provisorisk reglering av behandling av personuppgifter inom domstolarnas verksamhet.

Efter mer ingående överväganden lämnade utredningen därefter i december 2001 ett slutligt förslag på reglering av behandling av personuppgifter i domstolarnas rättsskipande och rättsvårdande verksamhet. Detta förslag är alltjämt föremål för beredning i Regeringskansliet. Domstolarnas behandling av personuppgifter regleras alltså sedan flera år tillbaka av tre förordningar av närmast provisorisk karaktär. Arbetsdomstolen och Marknadsdomstolen är inte föremål för någon särskild reglering, utan dessa domstolars behandling av personuppgifter regleras i personuppgiftslagen. Detta förefaller inte vara en tillfredsställande ordning, bland annat beroende på av att domstolarna torde bedriva sådan verksamhet att de har behov av att behandla känsliga personuppgifter i större utsträckning än vad personuppgiftslagen medger. Personuppgiftslagen kräver ju i princip samtycke vid behandling av känsliga personuppgifter. Om behandling skall få ske i större utsträckning än vad lagen medger krävs stöd i lag eller förordning (jfr 20 § PuL).

Regelverket förändras men de grundläggande principerna består

På domstolsområdet kommer inte sällan den enskildes intresse av skydd för sin personliga integritet i konflikt med ett annat grundläggande intresse, nämligen intresset av en rättssäker domstolsprocess och därmed också av allmänhetens förtroende för domstolarna. En rättssäker domstolsprocess har nämligen inte bara betydelse i det enskilda fallet, utan är också grundläggande för medborgarnas tillit till rättsväsendet i dess helhet. Sedan länge gäller fastslagna och tydliga regler på domstolsområdet beträffande hur avvägningen mellan intresset av offentlig insyn och enskildas intresse av skydd bör göras. Utgångspunkten är alltid att den rättskipande och rättsvårdande verksamheten i så stor utsträckning som möjligt skall ske under öppenhet. Särskilt framträdande är denna princip när det gäller de allmänna domstolarnas verksamhet. En annan hävdvunnen princip är att domstolarna ges stor frihet att i det enskilda fallet göra bedömningen huruvida insynsintresset eller den enskildes intresse av skydd väger tyngst.

Under senare tid har vissa ändringar i reglerna om sekretess på domstolsområdet skett. Dessa har inneburit såväl ett förstärkt skydd för enskildas intressen (uppgifter i mål om brott mot tystnadsplikt och dataintrång har getts primärt sekretesskydd hos domstolarna genom att föras in i 9 kap. 16 § SekrL) som ökad

öppenhet hos domstolarna (ändringen från omvänt till rakt skaderekvisit för uppgifter under förundersökning, 12 kap. 2 § andra stycket SekrL). Ändringarna kan inte anses innebära någon avvikelse från de väl etablerade principerna på domstolsområdet om hur avvägningen mellan intresset för offentlighet och enskilds intressen görs.

Någon närmare analys av huruvida regleringen av behandling av personuppgifter på domstolsområdet utgör ett tillfredsställande skydd för den personliga integriteten på domstolsrådet har inte gjorts, eftersom gällande reglering i form av tre förordningar är att betrakta som ett provisorium. Kommittén stannar vid att i detta sammanhang framhålla att behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet är av sådan karaktär och omfattning att de grundläggande principerna för behandlingen bör slås fast i lag. Att så ännu inte har skett kan inte anses tillfredsställande.

8.3.2 Vissa särskilda frågor av betydelse för skyddet för den personliga integriteten

Inledning

Även om regleringen på domstolsområdet rörande skyddet för uppgifter om enskilds personliga förhållanden förefaller bygga på sedan länge fastlagna och väl etablerade principer, har vissa farhågor framförts beträffande detta skydd i några enskilda frågor. En sådan fråga har att göra med utvecklingen mot och önskemålet om en moderniserad och mer effektiv domstolsprocess. Tvivel har också framförts i frågan om hotade och förföljda personers särskilda skyddsbehov är i tillräcklig mån tillgodosett. Nedan redogörs för dessa frågor.

Videoupptagning av förhör i domstol

Riksdagen antog den 16 juni 2005 regeringens förslag i proposition 2004/05:131 om förändringar av det processuella regelverket i syfte att uppnå en modernare rättegång i allmän domstol (bet. 2004/05:JuU29). Lagändringarna träder i kraft den dag regeringen bestämmer.

En av ändringarna innebär att en berättelse som lämnas i bevissyfte i tingsrätt skall dokumenteras genom en videoinspelning, om det inte finns särskilda skäl emot det. Som skäl anfördes bl.a. att antalet omförhör i hovrätt kan minska. Denna ändring har ansetts innebära vissa problem från integritetssynpunkt. Ett antal remissinstanser, bl.a. Svea hovrätt, Göta hovrätt och Hovrätten för Övre Norrland, var emot att förslaget genomfördes utan en fördjupad analys av integritetsaspekterna. Regeringen menade emellertid att den rättsliga regleringen kunde utformas på ett sätt som både tillgodosåg skyddet för den enskildes personliga integritet och utgjorde ett hinder mot att fotograferingsförbudet i rättssalen kringgås (a. prop. s. 105 f.). De nu aktuella ändringarna innebär att sekretess gäller för bilduppgiften i en videoupptagning som gjorts vid domstolsförhör. Sekretessen gäller, om det inte står klart att uppgiften kan röjas utan att den hörde lider men. Sekretessen består även om upptagningen spelas upp vid en offentlig förhandling. Vissa remissinstanser kritiserade denna ordning, eftersom man ansåg att det stred mot den systematik som reglerar förhållandet mellan sekretess och förhandlingsoffentlighet.

Möjlighet att hemlighålla skyddade personuppgifter

En viktig fråga för en part vars personuppgifter är skyddade i folkbokföringen är huruvida domstolen har möjlighet att hemlighålla dessa uppgifter i den mån de kommer att dokumenteras hos domstolen. Om uppgifterna kommer från en annan myndighet där sekretess för uppgifterna råder uppstår inget problem, eftersom sekretessen då överförs genom 12 kap. 1 § SekrL. Problem uppstår när en enskild, t.ex. parten själv, lämnar de skyddade uppgifterna till domstolen.

Problemet behandlades av Offentlighets- och sekretesskommittén i betänkandet *Ny sekretesslag* (SOU 2003:99, s. 180 f), där man föreslog att sekretess skall gälla inom hela den offentliga förvaltningen för uppgift om enskilds adress eller hemtelefonnummer eller annan liknande uppgift, om det av särskild anledning kan antas att den enskilde eller någon närstående kan komma att utsättas för hot, våld eller annat allvarlig men om uppgiften röjs. Förslaget var alltså utformat som en primär sekretessbestämmelse som blev tillämplig hos alla myndigheter. Det spelade därmed ingen

roll hur adressuppgiften hade hamnat hos myndigheten. Förslaget skulle ha inneburit ett förbättrat skydd för hotade och förföljda personers adressuppgifter och andra liknande uppgifter hos domstolarna.

Den 1 oktober 2006 infördes ändringar i 7 kap. sekretesslagen i huvudsakligen i enlighet med Offentlighets- och sekretesskommitténs förslag. Ändringarna innebär en möjlighet att sekretessbelägga skyddade personuppgifter inom hela den offentliga förvaltningen (prop. 2005/06:161, bet. 2005/06:KU35).

Offentlighets- och sekretesskommittén ansåg också att det på sikt finns skäl att generellt undersöka vilken rätt till partsinsyn som rättegångsbalken ger i olika fall. En särskilt viktig fråga i det sammanhanget var enligt kommittén partsinsynen i förhållande till skyddade personuppgifter. Denna del av kommitténs förslag bereds alltjämt i Regeringskansliet.

Sekretessbeläggning av namn i häktningsbeslut och andra icke slutliga beslut

Ett speciellt problem beträffande skydd hos domstolarna för uppgift om enskilds personliga förhållanden rör möjligheterna att hemlighålla den misstänktes namn i häktningsbeslut och andra beslut, t.ex. i ett beslut om förordnande av offentlig försvarare. Enligt 12 kap. 4 § andra stycket SekrL får förordnande om att sekretessen i ett mål skall bestå inte omfatta domslutet eller motsvarande del av annat beslut. I förarbetena till sekretesslagen sägs att det får förutsättas att domstolarna är restriktiva vid sekretessbeläggning av domar och beslut (prop. 1979/80:2 Del A s. 309). Vad som åsyftas med uttrycket ”domslutet eller motsvarande del av annat beslut” har dock inte berörts särskilt.

JO har i ett beslut (JO 2004/05 s. 42) ansett att den tolkning som ligger närmast till hands är att lagstiftaren avsett inte bara slutliga beslut utan åtminstone också vissa icke slutliga beslut. Ett förfarande, som innebär att man av hänsyn till den enskildes integritet inte låter den misstänktes identitet framgå av ett beslut om förordnande av försvarare, kunde enligt JO inte anses på ett oacceptabelt sätt komma i konflikt med offentlighets- och säkerhetsintressena. När det gäller frågan om den misstänktes namn kan hemlighållas även i ett häktningsbeslut intog JO dock motsatt hållning. JO underströk att ett häktningsbeslut medför

ingripande rättsverkningar för den enskilde, att ett sådant beslut fattas vid en förhandling och att andra jämförbara beslut om frihetsberövanden är offentliga. Mot den bakgrunden ansåg JO att 12 kap. 4 § andra stycket SekrL skall ges innebörden att den del av beslutet som inte får hemlighållas skall innehålla tydliga uppgifter om den frihetsberövade personens identitet. JO ansåg således att 12 kap. 4 § andra stycket SekrL inte ger möjlighet att under hänvisning till exempelvis 5 kap. 1 § eller 9 kap. 17 § SekrL hemlighålla uppgiften om den misstänktes identitet i ett beslut som innebär att denne häktas. Att den misstänkte själv framfört önskemål om att hans identitet inte skall röjas saknade enligt JO härvid betydelse. JO framhöll att rättsläget i denna fråga emellertid knappast var helt klart.

Frågan är inte föremål för överväganden i någon utredning, men har uppmärksammats inom Regeringskansliet. Den berördes i proposition 2003/04:93 om några frågor om sekretess (s. 66 f.), där man bl.a. redogjorde för det ovan nämnda JO-beslutet.

9 Straffprocessuella tvångsmedel

Huvudsaklig bedömning:

– Genom lagstiftning som trädde i kraft den 1 oktober 2004 frångicks krav som dittills under lång tid ansetts grundläggande vid användningen av hemliga tvångsmedel. Denna lagstiftning genomfördes utan att nya och eller tidigare okända omständigheter åberopades för den utvidgade tvångsmedelsanvändningen och utan att konsekvenserna för den enskildes integritet analyserades tillräckligt.
– Den parlamentariska kontrollen av användningen av de hemliga tvångsmedlen är svag och bedrivs inte effektivt.
– Systemet med offentliga ombud bör följas upp på ett mer gediget sätt än vad som hittills skett.
– Den rättsliga verkan av den enskildes samtycke till kroppsvisitation och kroppsbesiktning, däribland tagande av DNA-prov, bör klargöras genom lagreglering.
– I underlaget för de vilande förslagen om buggning och preventiv tvångsmedelsanvändning finns ingen närmare analys av konsekvenserna för den enskildes integritet. I lagstiftningsärendet om buggning täcker den behovsredovisning som finns tillgänglig bara delvis det föreslagna tillämpningsområdet. Beträffande båda förslagen synes därför underlaget behöva kompletteras för att det skall bli möjligt att göra en sådan proportionalitetsbedömning som enligt såväl regeringsformen som Europakonventionen utgör en förutsättning för en rättighetsbegränsande lagstiftning.

9.1 Myndighetsorganisationen

De brottsutredande myndigheterna utgörs i första hand av polisen och åklagare. Till polisens uppgifter hör att förebygga brott samt bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Polisen skall också förebygga och övervaka allmän ordning och säkerhet samt hindra och ingripa vid störningar. Till åklagares uppgifter hör att ansvara för ledningen av alla kvalificerade brottsutredningar där det finns en skälig brottsmisstanke mot någon. Åklagare skall också besluta i åtalsfrågor och föra det allmännas talan i brottmålsprocesser.

Även andra myndigheter kan medverka i brottsutredningar. Det gäller t.ex. Skatteverket, Kronofogdemyndigheten och Tullverket. Dessa myndigheter får dock som huvudregel inte verkställa beslut om tvångsmedel. Medverkan av andra myndigheter än polisen i den brottsbekämpande verksamheten kommer inte att behandlas här utan i samband med respektive kartläggningsområde.

Rikspolisstyrelsen är central förvaltningsmyndighet för polisväsendet och har tillsyn över detta. Till Rikspolisstyrelsen hör bl.a. Rikskriminalpolisen och Säkerhetspolisen.

Rikskriminalpolisen är den organisation inom vilken kampen mot den organiserade brottsligheten samordnas på central nivå. Inom Rikskriminalpolisen bedrivs bl.a. kriminalunderrättelsetjänst och vissa kvalificerade brottsutredningar rörande t.ex. våldsbrott, seriebrott, narkotikabrott och ekonomisk brottslighet. Rikskriminalpolisen ansvarar också för det operativa internationella polissamarbetet och för utvecklingsarbetet när det gäller internationella operativa frågor på kriminalpolisområdet. Säkerhetspolisen leder polisverksamhet för att förebygga eller avslöja brott mot rikets säkerhet. Det är också Säkerhetspolisens uppgift att leda polisverksamhet när det gäller bl.a. terroristbekämpning och bevaknings- och säkerhetsarbete som avser den centrala statsledningen eller som har samband med statsbesök och liknande händelser.

Den lokala polisorganisationen utgörs av en polismyndighet i varje län. Normalt finns vid en polismyndighet en polisoperativ enhet som i regel rymmer utredningsverksamhet, utryckningsverksamhet och trafikpolisverksamhet samt en förvaltningsenhet för bl.a. administrativa uppgifter. Alla polismyndigheter har kriminalunderrättelseenheter.

Åklagarorganisationen är sedan den 1 januari 2005 samlad inom en myndighet, *Åklagarmyndigheten.* Riksåklagaren är högste chef över åklagarväsendet och utövar tillsyn över åklagarverksamheten. Den operativa åklagarverksamheten bedrivs vid landets 43 åklagarkammare. Dessa har vanligtvis ett visst geografiskt arbetsfält.

9.2 Kort om regelverket

9.2.1 Vissa huvuddrag

Möjligheterna att använda tvångsmedel under förundersökning regleras av bestämmelserna i 24–28 kap. RB. Enligt JO innebär ett beslut om användning av sådant tvångsmedel att en förundersökning är eller skall anses vara inledd (JO 2001/02 s 89).

I den öppna polisens verksamhet får tvångsmedel användas endast under en förundersökning (för Säkerhetspolisen finns undantag från detta, se avsnitt 12.3). Förfarandet vid förundersökning är reglerat i rättegångsbalken och i förundersökningskungörelsen. Enligt 23 kap. 1 och 3 §§ RB skall polismyndighet eller åklagare fatta beslut om förundersökning så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. I 23 kap. 2 § RB sägs att förundersökningen har två huvudsakliga syften. Det ena syftet är att utröna om brott föreligger och vem som skäligen kan misstänkas för brottet samt att skaffa tillräckligt material för bedömning av frågan om åtal skall väckas. Det andra syftet är att bereda målet så att bevisningen kan förebringas i ett sammanhang vid huvudförhandlingen.

Mot bakgrund av hur de integritetsskyddande bestämmelserna i regeringsformen är utformade anses främst fyra allmänna principer gälla för användande av tvångsåtgärder mot enskilda. Dessa principer är legalitets-, ändamåls-, behovs- och proportionalitetsprinciperna.

Legalitetsprincipen finns direkt uttryckt i 2 kap. 12 § RF och innebär att sådana tvångsåtgärder som t.ex. kroppsligt ingrepp och husrannsakan inte får företas utan att det föreligger ett uttryckligt stöd i lag.

Även de tre övriga allmänna principerna anknyter till innehållet i 2 kap. 12 § RF.

Ändamålsprincipen innebär att en myndighets befogenhet att använda tvångsmedel skall vara bunden till det ändamål för vilket tvångsmedlet har beslutats. Om tvångsmedel avsiktligt används i annat syfte än det avsedda, kan det utgöra brott vid myndighetsutövning.

Behovsprincipen innebär att en tvångsåtgärd inte bör företas, om det inte är nödvändigt med hänsyn till syftet med åtgärden. Om flera alternativa medel står till buds för att uppnå det eftersträvade målet skall det medel väljas som innebär minsta möjliga intrång i den enskildes frihet och rätt. Åtgärden bör i varje enskilt fall vara ägnad att leda till det önskade resultatet. När det inte längre föreligger skäl för åtgärden skall den upphävas.

Proportionalitetsprincipen innebär att ett tvångsmedel får tillgripas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. Tvångsåtgärden skall alltså i fråga om art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden. Proportionalitetsprincipen fick år 1989 komma till direkt uttryck i lagtexten rörande de olika tvångsmedlen i 24–28 kap. RB. Den hade dock även dessförinnan ansetts gälla sedan länge enligt mer eller mindre underförstådda rättsgrundsatser.

Tvångsmedlen kan delas in i *personella* och i *reella* tvångsmedel. Till de personella tvångsmedlen hör de som riktar sig mot personen i fråga, t.ex. häktning och anhållande (24 kap. RB). De reella tvångsmedlen tar sikte på den enskildes egendom och syftar till att inskränka den vanliga förfoganderätten över egendomen. Exempel på reella tvångsmedel är kvarstad (26 kap. RB), beslag (27 kap. 1–17 §§) och husrannsakan (28 kap. 1–10 §§). Till de reella tvångsmedlen räknas också hemlig teleavlyssning och hemlig teleövervakning (27 kap. 18–30 §§ RB) samt hemlig kameraövervakning, som regleras särskilt i lagen (1995:1506) om hemlig kameraövervakning. Kartläggningen har endast tagit sikte på de reella tvångsmedlen.

9.2.2 Hemliga tvångsmedel

En annan indelning som kan göras i användningen av tvångsmedel är *hemliga* respektive *öppna* tvångsmedel. De hemliga tvångsmedel som för närvarande tillåts i svensk rätt är hemlig teleavlyssning och

hemlig teleövervakning, som regleras i 27 kap. RB, samt hemlig kameraövervakning, som regleras särskilt i lagen (1995:1506) om hemlig kameraövervakning. När det gäller åtgärder riktade mot ”vanlig” brottslighet, dvs. sådana som inte omfattas av säkerhetstjänstens område, är hemlig teleavlyssning det äldsta tvångsmedlet, och företeelsen har varit reglerad sedan 1940-talet. Hemlig teleövervakning blev reglerad i rättegångsbalken år 1989. Redan lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål, som alltjämt är tillämplig i Säkerhetspolisens verksamhet, innehöll dock bestämmelser härom. Regler som tillåter användning av hemlig kameraövervakning infördes år 1996 i form av en tidsbegränsad men ännu gällande lag.

Regeringen lade våren 2006 fram förslag till utvidgade möjligheter att använda hemliga tvångsmedel i form av ett nytt tvångsmedel benämnt *hemlig avlyssning* (buggning). Samtidigt föreslogs att hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning och postkontroll skulle få användas i syfte att förebygga brott. De nya möjligheterna att använda tvångsmedel föreslogs införde genom särskilda lagar. Riksdagen beslutade den 31 maj 2006 med stöd av 2 kap. 12 § tredje stycket RF att de båda lagförslagen skulle vila i minst ett år.

I utredningsbetänkandet *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98) föreslås att det skall införas en särskild skyldighet att underrätta enskilda personer som har påtagligt berörts av sådan verkställighet av hemliga tvångsmedel som sker i brottsutredningar.

En mer utförlig redovisning av gällande regler för användning av hemliga tvångsmedel ges i kapitel 28. Där lämnas också en historik över hur lagstiftningen beträffande de hemliga tvångsmedlen har utvecklats. I detta sammanhang redovisas också de nu vilande förslagen om utvidgad användning av hemliga tvångsmedel i form av buggning och användning i förebyggande syfte. Även utredningsförslaget om en underrättelseskyldighet redovisas där.

9.2.3 Öppna tvångsmedel

Till de öppna straffprocessuella tvångsmedlen hör beslag, husrannsakan, kroppsvisitation och kroppsbesiktning. Beslag regleras i 27 kap. RB och de övriga nämnda tvångsmedlen i 28 kap. RB. Tvångsmedlet kroppsbesiktning innefattar tagande av DNA-prov.

Från brottsutredningssynpunkt är en viktig del i användningen av detta tvångsmedel den registrering av uppgifter från DNA-prov som sker. Regler rörande sådan registrering behandlas i kapitel 11.

En mer utförlig redovisning av gällande regler för användning av de ovan nämnda öppna tvångsmedlen lämnas i kapitel 28. Där redovisas också regler som rör möjligheterna att ta fotografi och fingeravtryck av häktade och anhållna.

Lagstiftningen rörande de öppna tvångsmedlen har i sina huvuddrag varit i stort sett oförändrad under årens lopp. Någon historik över hur lagstiftningen har förändrats lämnas därför inte.

9.2.4 Andra metoder av betydelse för brottsutredningen

Lagring av uppgifter och uppgiftsskyldighet hos teleoperatörer

Av betydelse för den brottsutredande verksamheten är också möjligheten att från teleoperatörer hämta in uppgifter om teletrafik enligt 6 kap. 22 § lagen (2003:389) om elektronisk kommunikation samt, om den som bedriver televerksamhet är en myndighet, enligt 14 kap. 2 § fjärde och femte styckena SekrL. Denna möjlighet behandlas i kapitel 15.

Där redovisas också det nyligen antagna EG-direktivet om lagring av trafikuppgifter, som innebär att teleoperatörer och innehavare av elektroniska kommunikationsnät åläggs en skyldighet att lagra trafikuppgifter för brottsbekämpningsändamål. Uppdraget till den utredning som skall lämna förslag till direktivets genomförande i svensk lagstiftning redovisas också.

Tekniska spaningsmetoder

Under en förundersökning, men vanligare under det spaningsskede som föregår en förundersökning, kan åtgärder sättas in som brukar benämnas ”okonventionella spaningsmetoder” (i kommitténs direktiv används beteckningen ”övervakningsmetoder”). Det kan röra sig om användning av dold kroppsmikrofon eller handmanövrerad kamera, inspelning av telefonsamtal eller positionsbestämning (s.k. pejling). Några särskilda regler för rätten att använda denna typ av arbetsmetoder finns inte. Däremot finns i 8 § polislagen (1984:387) en allmän bestämmelse om att en polisman som har att verkställa en tjänsteuppgift under iakttagande av vad

som föreskrivs i lag eller annan författning skall ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Användningen av polisens spaningsmetoder behandlas närmare i kapitel 10.

9.2.5 Internationella överenskommelser

Sverige har ingått flera överenskommelser om rättslig hjälp i brottmål både inom och utom EU. En grundläggande sådan överenskommelse inom Europa är den europeiska konventionen om ömsesidig rättslig hjälp i brottmål (ETS 030) som antogs år 1959.

I lagen (2000:562) om internationell rättslig hjälp finns bestämmelser om i vilka fall straffprocessuella tvångsmedel kan aktualiseras i Sverige efter ansökan från annan stat.

En närmare redogörelse för 1959 års konvention och andra internationella överenskommelser, samt för lagen om internationell rättslig hjälp lämnas i kapitel 28.

9.3 Kontroll av de hemliga tvångsmedlens användning

9.3.1 Den parlamentariska kontrollen

Bakgrund

Riksdagen framställde under riksmötet 1981/82 önskemål om att regeringen årligen skulle redovisa hur reglerna om teleavlyssning i rättegångsbalken har tillämpats. Regeringen lämnade första gången en sådan redovisning vid riksmötet 1983/84 (skr. 1983/84:97). Bakgrunden till riksdagens önskemål var att regeringen tidigare i samband med årliga propositioner om förlängning av lagen (1969:36) om telefonavlyssning vid förundersökning angående grovt narkotikabrott m.m. hade lämnat en redogörelse för tillämpningen av lagen. Efter det att lagen upphört att gälla år 1981 och motsvarande möjlighet att ge tillstånd till telefonavlyssning införts i rättegångsbalken, lämnades ingen redovisning till riksdagen på sätt som skett tidigare.

Under riksdagsärendets behandling anförde justitieutskottet (bet. JuU 1981/82:54) att det var angeläget att riksdagens möjligheter till insyn i fråga om telefonavlyssning vidmakthölls och, om möjligt, byggdes ut. Insynen borde ske i form av en årlig redo-

visning i proposition eller skrivelse till riksdagen. Den borde såsom dittills avse telefonavlyssning enligt den tidsbegränsade lagen (1975:1360) om tvångsåtgärder i spaningssyfte i vissa fall, den s.k. spaningslagen, eller motsvarande lagstiftning och vid förundersökning angående grovt narkotikabrott och grov varusmuggling av narkotika samt därjämte övrig telefonavlyssning enligt de grundläggande reglerna i RB. Utskottet ansåg, med hänvisning till vad 1974 års utredning om telefonavlyssning anfört i betänkandet *Telefonavlyssning* (SOU 1975:95 s. 103 f.), att redovisningen borde kunna ge riksdagen en uppfattning om bl.a. antalet ärenden om telefonavlyssning, antalet meddelade tillstånd, vilka tillståndstider som förekommit samt i vilken mån telefonavlyssningen fyllt avsett ändamål. I övrigt borde redovisningen i huvudsak utformas efter mönster av de redogörelser som riksdagen dittills fått. I fråga om redovisning av telefonavlyssning beträffande sådana brottmål som avses i 1952 års tvångsmedelslag förordade utskottet ingen ändring i förhållande till den ditintills gällande ordningen, som bland annat innebar att vederbörande utskott självt kunde inhämta den information som ansågs behövlig.

I samband med att reglerna om hemlig teleavlyssning och hemlig teleövervakning ändrades år 1989 uttalades att regeringens redovisning till riksdagen angående tillämpningen av bestämmelserna om hemlig teleavlyssning borde bibehållas och att en motsvarande redovisning beträffande hemlig teleövervakning borde lämnas (prop. 1988/89:124 s. 55). Även i det lagstiftningsärende som låg till grund för lagen (1995:1506) om hemlig kameraövervakning uttalades att en redovisning av tillämpningen av bestämmelserna i den lagen skulle lämnas (prop. 1995/96:85 s. 37).

Redovisningen till riksdagen

Inledning

De årliga redovisningarna till riksdagen avser den öppna polisens tillämpning av reglerna om hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken och om hemlig kameraövervakning enligt lagen om hemlig kameraövervakning. Senast lämnades en sådan redovisning vid riksmötet 2006/07 och avsåg lämnade tillstånd under år 2005 (skr. 2006/07:28).

Frågor om insyn i användningen av hemliga tvångsmedel enligt 1952 års tvångsmedelslag behandlas i samband med kartläggningen av området för säkerhetstjänsten (se kapitel 12).

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns även i lagen (1991:572) om särskild utlänningskontroll. En redogörelse för tillämpningen av lagen lämnas årligen av regeringen till riksdagen genom en skrivelse. Detta skedde senast vid riksmötet 2006/07 (skr. 2006/07:18).

Redogörelsen nedan omfattar således endast den öppna polisens användning av hemliga tvångsmedel enligt rättegångsbalken och enligt lagen om hemlig kameraövervakning.

Redovisningens innehåll

I regeringens skrivelse till riksdagen lämnas separata redovisningar för de olika slagen av hemliga tvångsmedel. Redovisningarna bygger i huvudsak på uppgifter som Åklagarmyndigheten och Rikspolisstyrelsen gemensamt har lämnat till regeringen.

Beträffande användningen av de hemliga tvångsmedlen lämnades i den senaste skrivelsen uppgifter om

- det totala antalet lämnade tillstånd
- antalet meddelade tillstånd i förundersökning rörande grovt narkotikabrott eller grov narkotikasmuggling,
- antalet meddelade tillstånd som avsett annan brottslighet och vad denna brottslighet rört för typ av brott,
- den genomsnittliga avlyssnings/övervakningstiden,
- andelen fall då avlyssningen/övervakningen ”haft betydelse för förundersökningen beträffande den misstänkte”,
- andelen fall då förundersökningen lagts ned på grund av att brott inte kunnat styrkas,
- andelen fall då avlyssningen/övervakningen av andra skäl inte tjänat sitt syfte,
- antalet fall då ansökan om hemlig teleavlyssning/teleövervakning avslagits,
- antalet fall då tillstånd till teleavlyssning/övervakning meddelats efter begäran om rättslig hjälp från annat land.

Redogörelsen innehöll också statistiska uppgifter i form av stapeldiagram för den senaste tioårsperioden avseende dels antalet tillstånd som rört grovt narkotikabrott eller grov narkotikasmuggling, dels antalet tillstånd som rört annan brottslighet, dels den genomsnittliga avlyssnings- respektive övervakningstiden, dels andelen fall där åtgärden haft betydelse för förundersökningen.

En sammanställning över tid av meddelade tillstånd för användning av hemliga tvångsmedel redovisas i kapitel 28.

Riksdagens behandling

Riksdagens behandling av regeringens skrivelse om tillämpningen av reglerna om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning har i allmänhet avslutats med att skrivelsen lagts till handlingarna som enda åtgärd. Under senare år har dock förekommit att riksdagen gjort ett tillkännagivande till regeringen som rört redovisningens innehåll (se bet. 2005/06:JuU12).

Skrivelsen har tidigare i allmänhet inte föranlett några motioner. Under senare år har motioner dock vanligtvis förekommit. Den fråga som mer än andra väckt intresse i samband med behandlingen av regeringens skrivelse har rört riksdagens möjligheter till insyn i hur reglerna om de hemliga tvångsmedlen har tillämpats. Regeringens redogörelse var från början mer knapphändig. Den första redogörelsen från riksmötet 1983/84, som enbart avsåg hemlig telefonavlyssning, innehöll uppgifter om antalet meddelade tillstånd i förundersökning som rört grovt narkotikabrott eller grov narkotikasmuggling respektive i förundersökning beträffande annat brott. En redovisning lämnades också av antalet meddelade tillstånd i förundersökning rörande grova narkotikabrott eller grov varusmuggling under åren 1969–1982. Dessutom lämnades upplysningen att ”flertalet fall av avlyssning leder till att den avlyssnade döms till frihetsberövande åtgärd”.

I samband med behandlingen av skrivelsen 1984/85:104 erinrade justitieutskottet om sitt uttalande år 1982 i frågan om vilka möjligheter till insyn för riksdagen som redovisningens innehåll ger (bet. JuU 1984/85:17). Utskottet framhöll att det vid en hearing i ärendet med företrädare för Justitiedepartementet och Rikspolisstyrelsen uppgivits att överväganden pågick inom den sistnämnda myndigheten i syfte att – i linje med utskottets uttalande – åstad-

komma en utbyggd redogörelse för tillämpningen. Vid riksmötet 1986/87 återkom utskottet på nytt till denna fråga och erinrade om vikten av att redovisningen till regeringen och till riksdagen tillgodosåg de anspråk som riksdagen ställde upp år 1982 (bet. JuU 1986/87:12). Det sagda gällde inte minst uppgifter om vilka tillståndstider som förekommit och i vilken mån telefonavlyssningen fyllt avsett ändamål. Någon åtgärd från riksdagens sida påfordrades dock enligt utskottet inte, eftersom Rikspolisstyrelsen ställt i utsikt att redovisningen för år 1985 skulle komma att byggas ut. Utskottet fick dock anledning att på nytt upprepa sina önskemål vid det därpå följande riksmötet (bet. JuU 1988/87:4). Vid sin behandlingen av skrivelsen under riksmötet 1990/91 och en i anledning härav väckt motion, som rörde frågan om riksdagens möjlighet till insyn, konstaterade justitieutskottet att redovisningarna numera innehöll även de kvalitativa element som tidigare efterlysts och att redogörelserna uppfyllde de krav som riksdagen, efter ingående överväganden, uppställt (bet. 1990/91:JuU6).

Frågan huruvida redovisningen i den årliga skrivelsen borde förbättras har behandlats flera gånger också under senare år. I skrivelse 2001/02:52 avseende lämnade tillstånd under år 2000 anförde regeringen att redovisningen delvis byggde på uppgifter som kan vara svåra att bedöma (s. 13). Som exempel kunde nämnas frågan om ett meddelat tillstånd haft betydelse för förundersökningen eller inte. Bedömningen gjordes vid denna tidpunkt av respektive polismyndighet utan stöd av enhetliga riktlinjer. Regeringen avsåg att genom en dialog med myndigheterna undersöka om redovisningen kunde förbättras i syfte att stärka förutsättningarna för den parlamentariska granskningen. Vissa mindre förändringar av redovisningen har därefter skett, bland annat lämnas numera också uppgift om antalet tillstånd som meddelats efter begäran om rättslig hjälp från annat land. Även riksdagen har under senare år återkommande behandlat frågan om en förbättrad redovisning. Detta skedde senast i samband med behandlingen av skrivelse 2005/06:53 (bet. 2005/06:JuU12), då flera motioner berörde denna fråga. Utskottet anförde att regeringens arbete med att förbättra redovisningen hade pågått i flera år, dock utan att någon nämnvärd förbättring skett. En tydlig och snar förändring av redovisningens innehåll var enligt utskottet nödvändig för att riksdagen skall kunna utföra sin granskningsuppgift.

Förslag om en förstärkt parlamentarisk kontroll

Justitiedepartementet gav den 22 juni 2005 en särskild utredare i uppdrag att presentera förslag på hur den parlamentariska kontrollen när det gäller de brottsbekämpande myndigheternas användning av hemliga tvångsmedel kan stärkas. Förslaget skulle även omfatta användningen av hemliga tvångsmedel i ärenden som initieras eller handläggs av Säkerhetspolisen.

Resultatet av uppdraget redovisades i november 2005 genom promemorian *Hemliga tvångsmedel m.m. under stärkt parlamentarisk kontroll* (Ds 2005:53). I promemorian föreslogs att en särskild nämnd inrättas under regeringen med uppgift att utöva tillsyn över myndigheternas användning av hemliga tvångsmedel. I nämndens uppgift skulle ingå att granska tillämpningen av bl.a. reglerna i rättegångsbalken, lagen om hemlig kameraövervakning och 1952 års tvångsmedelslag. Granskningen skulle avse användningen av de hemliga tvångsmedlen samt postkontroll och överskottsinformation.

Vid remissbehandlingen av promemorian förordade flertalet remissinstanser en stärkt insyn och kontroll av användningen av tvångsmedel, men avstyrkte att den föreslagna tvångsmedelsnämnden inrättades. Man ansåg att förslaget inte innebar en förstärkt parlamentarisk kontroll, utan tvärtom en försvagning av denna. Vidare ansåg man att den föreslagna nämndens förhållande till JO:s och JK:s granskning inte hade utretts.

Utredningen om rättssäkerhet vid hemliga tvångsmedel föreslår i betänkandet *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel* (SOU 2006:98) att det under regeringen inrättas en nämnd, Säkerhets- och integritetsskyddsnämnden, med stark parlamentarisk anknytning. Enligt utredningen förutsätter dess förslag om en särskild skyldighet att underrätta enskilda om användning av hemliga tvångsmedel att det inrättas ett oberoende organ med uppgift att granska den verksamhet där det förekommer användning av hemliga tvångsmedel. Utredningen anser vidare att rättssäkerheten för enskilda skulle förstärkas väsentligt om det införs en efterhandskontroll av användandet av hemliga tvångsmedel som kompletterar den kontroll i förhand som i dag utövas av domstolarna. Nämndens löpande tillsyn skall utföras genom inspektioner och andra undersökningar. Därtill föreslås nämnden få handlägga särskilda kontrollärenden på begäran av enskilda.

9.3.2 Offentliga ombud

Inledning

Sedan den 1 oktober 2004 skall rätten förordna ett offentligt ombud i ärenden om hemlig teleavlyssning och hemlig kameraövervakning. Ombudets uppgift är inte att företräda den misstänkte i det enskilda fallet, utan att företräda enskildas rätt och integritetsintressen i allmänhet. Av den anledningen förordnas ombudet inte för den misstänkte eller för någon annan särskild person. Ombudet skall ha tillgång till allt material i tvångsmedelsärendet och har möjlighet att överklaga rättens beslut.

Om ett ärende är så brådskande att det inte finns tid att förordna ett offentligt ombud, får ett sammanträde hållas och beslut fattas utan att något offentligt ombud varit närvarande eller annars fått tillfälle att yttra sig.

I ärenden om hemlig teleövervakning förordnas inget offentligt ombud. Behovet av offentliga ombud har i dessa ärenden ansetts mindre (prop. 2003/04:74 s 23 f.). Eftersom frågan om att avskaffa möjligheten att inhämta teleövervakningsuppgifter direkt från teleoperatör skulle ses över borde enligt regeringen ett ställningstagande i frågan om medverkan av offentligt ombud i ärenden om hemlig teleövervakning anstå till dess att en sådan översyn var slutförd. Den nämna översynen har numera genomförts av Beredningen för rättsväsendets utveckling, som i sitt betänkande *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38) föreslår att de brottsutredande myndigheternas tillgång till uppgifter från teleövervakning enbart skall regleras i 27 kap. RB. Beredningen berör dock inte frågan om medverkan av offentligt ombud i dessa ärenden.

Bakgrund

Frågan om att införa en slags motpart till åklagaren i form av en god man, offentligt ombud eller liknande i ärenden om hemliga tvångsmedel har behandlats tidigare i flera sammanhang. I proposition 1975/76:202 föreslogs att reglerna i 1952 års tvångsmedelslag och i 1969 års lag om telefonavlyssning vid förundersökning angående grovt narkotikabrott m.m. skulle permanentas och samordnas i 27 kap. RB. I detta sammanhang lämnades också förslag som syftade till att i olika avseenden stärka skyddet för den enskildes

integritet, bl.a. i form av ett antal av regeringen utsedda gode män. Förslagen i propositionen genomfördes inte (bet. JuU 1976/77: 20).

Även Tvångsmedelskommittén föreslog i betänkandet *Tvångsmedel Anonymitet Integritet* (SOU 1984:54) att en ordning med offentligt ombud skulle införas i fråga om bl.a. telefonavlyssning, beslag och husrannsakan. Regeringen ställde sig dock inte bakom kommitténs förslag i denna del i proposition 1988/89:124.

Frågan om en ordning med offentliga ombud behandlades också av SÄPO-kommittén i betänkandet *Säkerhetspolisens arbetsmetoder, personalkontroll och meddelarfrihet* (SOU 1990:51 s. 175 f.). Kommittén avvisade tanken på ett sådant ombud och åberopade därvid i huvudsak samma skäl som regeringen i proposition 1988/89:124. Ett system med ombud skulle enligt kommittén närmast kunna betecknas som en skenprocess där några avgörande fördelar inte stod att vinna.

Buggningsutredningen föreslog i betänkandet *Om buggning och andra hemliga tvångsmedel* (SOU 1998:46) att ett offentligt ombud skulle utses både i ärenden om de befintliga tvångsmedlen hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning samt i ärenden om de av utredningen föreslagna tvångsmedlen hemlig avlyssning (buggning) och annan teknisk avlyssning. I lagrådsremissen *Hemlig avlyssnin*g (Ju98/1450) lade regeringen fram förslag till lagändringar som i sina huvuddrag stämde överens med Buggningsutredningens förslag.

Aktuell situation

I augusti 2004 förordnade regeringen för första gången offentliga ombud enligt 27 kap. 27 § RB i ärenden om hemlig teleavlyssning och hemlig kameraövervakning. Förordnandena gäller fr.o.m. den 1 oktober 2004 t.o.m. den 30 september 2007.

De offentliga ombuden är förordnade länsvis. Stockholms län har det högsta antalet ombud, 11 st. För varje län har minst två ombud förordnats, utom för Värmlands län som endast har ett ombud. Sammanlagt har förordnats 76 offentliga ombud. Av dessa är 46 advokater och 30 domare. Av domarna är, såsom reglerna påbjuder, ingen längre verksam i ordinarie tjänst och huvuddelen av dem har haft en chefsbefattning.

Från Regeringskansliet har inhämtats att statistik saknas över i vilken utsträckning de offentliga ombuden har överklagat beslut att medge teleavlyssning eller kameraövervakning. Detsamma gäller i vilken utsträckning tvångsmedelsärenden har ansetts så brådskande att beslut har fattats utan att ett offentligt ombud förordnats.

Utredningen om rättssäkerhet vid hemliga tvångsmedel har i sitt betänkande *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98) gjort bedömningen att inga förändringar behövs i systemet med offentliga ombud. Utredarens slutsats att systemet fungerar väl synes främst baseras på uppgifter som lämnats vid ett samrådsmöte.

9.4 Kontroll av användningen av öppna tvångsmedel

9.4.1 Riksdagens ombudsmän

Från Riksdagens ombudsmän (JO) har inhämtats att klagomål avseende brottsutredande myndigheters handläggning av öppna tvångsmedel, som beslag, husrannsakan, kroppsvisitation och kroppsbesiktning, hör till de vanligare som JO har att hantera. Antalet ärenden där JO har haft anledning att komma med kritik har varit i stort sett oförändrat under årens lopp. Endast i ett fåtal fall har JO haft anledning att uttala sig om regleringen av de nu aktuella tvångsmedlen, och det har då handlat om vissa detaljfrågor.

9.4.2 Justitiekanslern

Justitiekanslerns (JK) hantering av klagomål rörande användning av öppna tvångsmedel uppvisar i stort sett samma bild som den som JO har beskrivit. Det är sålunda relativt vanligt med klagomål. I JK:s skadereglerande verksamhet har skadestånd för kränkning utgått i ett begränsat antal fall. Klagomålen har i allmänhet inte avsett att grund för användning av tvångsmedlet har saknats, utan att den brottsutredande myndigheten i något avseende inte har iakttagit vad som är föreskrivet för hur tvångsmedlet skall användas. Det kan t.ex. ha handlat om att ett beslag inte har hävts i rätt tid eller att en husrannsakan inte har genomförts på föreskrivet sätt.

9.4.3 Polismål

Från Riksenheten för polismål vid Åklagarmyndigheten har inhämtats att enheten tar emot ungefär 1100 klagomål per år som rör enskilda polismäns ageranden i samband med bl.a. användning av tvångsmedel. Ungefär 30 procent av dessa leder till att förundersökning inleds. När det gäller användningen av tvångsmedel enligt rättegångsbalken kan klagomålen inte härledas till problem med det gällande regelverket som sådant, utan klagomålen har sin grund i enskilda polismäns slarv eller att man helt enkelt har åsidosatt reglerna. De problem med regelverket som iakttagits rör i stället områden utanför den egentliga tvångsmedelsanvändningen, där annan reglering än de generellt tillämpliga behovs- och proportionalitetsprinciperna i stor utsträckning saknas och där det finns ”gråzoner” för vad som är rätt eller fel.

9.5 Sammanfattning och bedömning

9.5.1 Inledning

De straffprocessuella tvångsmedlen intar en särställning på integritetsskyddsområdet, såtillvida som de ger staten laglig rätt till en långtgående och ofta djupt integritetskränkande övervakning och kontroll av medborgarna. Särskilt gäller detta de hemliga straffprocessuella tvångsmedlen. Anledningen till att dessa tvångsmedel alls kan accepteras i ett demokratiskt samhälle är att motstående intressen, i synnerhet intresset av att effektivt kunna bekämpa grov brottslighet, under vissa omständigheter ter sig viktigare än skyddet för den personliga integriteten.

I det följande ges en översikt över de straffprocessuella tvångsmedlen. I anslutning härtill görs ett antal reflektioner och lämnas vissa, delvis kritiska synpunkter. Synpunkterna tar sikte dels på själva lagstiftningsprocessen, dels på kontrollen av tvångsmedlens användning. En beskrivning av och vissa synpunkter på aktuella förslag till framtida reglering lämnas också. De synpunkter som framförs innebär inte i något fall att ställning tas till huruvida ett visst tvångsmedel är godtagbart från integritetsskyddssynpunkt. En sådan bedömning kan inte göras isolerad för sig, utan förutsätter att hela problembilden kan överblickas, inklusive arten och omfattningen av den brottslighet som motiverar tvångsmedlen samt kännedom om hur denna brottslighet bäst och mest effektivt kan

bekämpas. Det är förvisso inte heller en uppgift för kommittén att överpröva nödvändigheten av de olika straffprocessuella tvångsmedlen. Däremot ligger det klart inom kommitténs uppdrag att granska hur väl integritetsskyddsaspekter har lyfts fram och beaktats i lagstiftningsprocessen liksom inom ramen för uppföljning och kontroll av tvångsmedelsanvändningen.

9.5.2 Grundläggande utgångspunkter för användning av straffprocessuella tvångsmedel

Europakonventionen

En grundläggande utgångspunkt för varje diskussion om i vilken utsträckning de straffprocessuella tvångsmedlen kan tillåtas inskränka den personliga integriteten är att Sverige måste iaktta de begränsningar som följer av landets anslutning till Europakonventionen och dess tilläggsprotokoll. Detta gäller i desto högre grad som konventionen sedan den 1 januari 1995 utgör en integrerad del av den svenska rättsordningen och åtnjuter grundlagsstatus såtillvida som regeringsformen innehåller ett förbud mot stiftande av konventionsstridiga lagar. Det bör observeras att konventionsåtagandet även innefattar en skyldighet att rätta sig efter den tolkning av konventionsbestämmelserna som framgår av Europadomstolens praxis.

Enligt artikel 8.2 i Europakonventionen får vars och ens rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens inte inskränkas annat än med stöd av lag och 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.

Europadomstolen har framhållit att kravet på att ingreppet skall vara nödvändigt inte är synonymt med ”oundgängligt” (Danelius, s. 264 f.) Vad som krävs är däremot att det finns ett ”angeläget samhälleligt behov”. Inskränkningen i den grundläggande rättigheten måste vidare stå i rimlig proportion till det syfte som skall tillgodoses genom inskränkningen. Varje konventionsstat har själv en viss frihet att avgöra om en inskränkning är nödvändig. Europadomstolen förbehåller sig dock rätten att övervaka om denna frihet utnyttjas på ett rimligt sätt.

Konventionsstaternas frihet att tolka konventionen är inte lika stor i fråga om alla de ändamål som anges i artikel 8:2. När det t.ex. är fråga om en inskränkning med hänsyn till statens säkerhet ges de nationella organen en mer vidsträckt frihet, något som har motiverats med att det här rör sig om ett intresse av fundamental betydelse för varje konventionsstat.

Regeringsformen

De fri och rättigheter som avses i bl.a. 2 kap. 6 § RF (rätt till skydd mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande) får enligt 2 kap. 12 § begränsas. Det får emellertid i så fall endast ske genom lag och bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En sådan rättighetsbegränsande lagstiftning får aldrig gå utöver vad som är nödvändigt med hänsyn till ändamålet och inte heller sträcka sig så långt att lagstiftningen utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar.

I förarbetena till regeringsformen betonades att regleringen i 2 kap. 12 § RF är ägnad att understryka kravet på att lagstiftaren, när en fri- och rättighetsinskränkande lag beslutas, noga redovisar sina syften (prop. 1975/76:209 s. 153).

9.5.3 Kommentar till gällande regler om hemliga tvångsmedel

Europadomstolen

Europadomstolen har i åtskilliga fall haft att bedöma i vad mån *telefonavlyssning* utgjort en konventionsenlig åtgärd. En första fråga har i dessa fall varit om ingreppet varit föreskrivet i lag. I flera fall har slutsatsen blivit att detta krav inte har varit uppfyllt. Förklaringen har ibland varit att det helt enkelt saknats lagstiftning. Vanligtvis har det dock funnits visst lagstöd, men bestämmelserna kan ha varit så oklara eller allmänt utformade att tillämpningen av dem inte varit i rimlig grad förutsebar (Danelius, s. 270 f.). I målen *Kruslin och Huvig,* båda mot Frankrike (24.4.1990), framhöll Europadomstolen att telefonavlyssning var ett allvarligt ingrepp i

rätten till privatliv och korrespondens och att tydligt lagstöd därför måste krävas. Det var viktigt att de regler som tillämpades var klara och detaljerade, något som inte ansågs vara fallet i dessa mål. Ett annat viktigt mål, där Europadomstolen behandlade problemen kring telefonavlyssning med syfte att skydda statens säkerhet, är *Klass m.fl. mot Tyskland* (6.9.1978). Europadomstolen berörde där särskilt behovet av kontroll av en åtgärd som vidtas utan att den närmast berörde i förväg informeras. Domstolen betonade att det måste finnas en effektiv kontroll av att systemet inte missbrukas.

Grundläggande element i den svenska regleringen fram till år 2004

De hemliga tvångsmedel som för närvarande tillåts i svensk rätt är hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning. När det gäller åtgärder riktade mot ”vanlig” brottslighet, dvs. sådana som inte omfattas av säkerhetstjänstens område, är hemlig teleavlyssning det äldsta tvångsmedlet, och företeelsen har varit reglerad sedan 1940-talet. Hemlig teleövervakning blev reglerad i rättegångsbalken år 1989. Redan lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål, som alltjämt är tillämplig i Säkerhetspolisens verksamhet, innehöll dock bestämmelser härom. Regler som tillåter användning av hemlig kameraövervakning infördes år 1996 i form av en tidsbegränsad men ännu gällande lag.

Fram till år 2004 kan följande grundläggande element i form av rättssäkerhetsgarantier och integritetsskydd sägas ha kännetecknat lagstiftningen:

- Tvångsmedlet är tillåtet endast inom ramen för en förundersökning, dvs. det måste ta sikte på ett redan begånget brott.
- Användningen av tvångsmedlet skall vara av synnerlig vikt för brottsutredningen.
- Det skall finnas någon som är skäligen misstänkt för brottet.
- Teleadressen/den övervakade platsen i fråga skall direkt kunna kopplas till den misstänkte.
- Beslut om användning av tvångsmedlet skall fattas av domstol.

Beträffande hemlig teleavlyssning och hemlig kameraövervakning, som brukar anses i stort sett likvärdiga när det gäller graden av integritetskränkning, har uppställts ett krav på att brottet skall ha så högt straffvärde att det kan rendera lägst två års fängelse.

När det gäller brott som *omfattas av säkerhetstjänstens område* har i vissa fall gjorts undantag från dessa grundläggande rättssäkerhets- och integritetsskyddskrav. Sådana avvikelser finns i 1952 års tvångsmedelslag, vilken tar sikte just på det område som säkerhetstjänsten har att bevaka, samt i lagar som avser terrorbrott eller som gäller i krigstid. I flera lagstiftningsärenden har det diskuterats om man skall släppa på något eller några av de nämnda grundläggande kraven också beträffande den så att säga ordinarie brottsbekämpningsverksamheten. Fram till år 2004 avvisades alla sådana tankegångar, bortsett från att en viss utvidgning av området för hemlig teleavlyssning har skett i och med att även förbrott till de brott som kan grunda tillstånd till avlyssning kom att omfattas av reglerna. Denna mer tekniskt betonade utvidgning av tvångsmedelsanvändningen kan dock knappast sägas ha inneburit något avsteg från de nämnda grundläggande kraven, inte ens i fråga om kravet på två års straffminimum.

2004 års reform

Den långvariga traditionen av vaktslående om krav som ansetts grundläggande vid användningen av hemliga tvångsmedel bröts genom lagstiftning som trädde i kraft den 1 oktober 2004. Då reformerades lagstiftningen om hemliga tvångsmedlen på ett sätt som innebar bl.a. följande.

- En s.k. straffvärdeventil infördes för hemlig teleavlyssning och hemlig kameraövervakning. Ändringen innebar beträffande kravet på två års fängelse att det räcker att strafftiden i det enskilda fallet kan antas överstiga två år. Tvångsmedlen kan alltså komma att tillgripas även i fall då minimistraffet för brottet väsentligt understiger två års fängelse.
- I fråga om hemlig teleavlyssning och hemlig teleövervakning släpptes kravet att det skall finnas en direkt koppling mellan teleadressen i fråga och den misstänkte. Avlyssning/övervakning kan därför numera ske av en teleadress *till* vilken den misstänkte ringer.

- Det dittillsvarande kravet på att det skall finnas någon skäligen misstänkt för brottet övergavs såvitt gäller hemlig kameraövervakning. Tillstånd till detta tvångsmedel kan sålunda numera lämnas även i de fall då det inte finns någon skäligen misstänkt.

Europakonventionens krav på att ett ingrepp i rätten till respekt för envars privat- och familjeliv etc. måste vara *nödvändigt* i ett demokratiskt samhälle, liksom regeringsformens motsvarande krav i fråga om rättighetsinskränkande lagstiftning, gäller inte bara då lagstiftning om att tillåta ett tvångsmedel införs, utan också vid varje utvidgning av ett tvångsmedels användningsområde eller då man i annat avseende medger lättnader i de krav som lagstiftningen ställer upp. Detta medför i sin tur ett krav på att det i ett lagstiftningsärende av det slaget finns en tillfredsställande redovisning av de behov som ändringen i reglerna förväntas fylla, så att det går att göra en på fakta grundad bedömning av hur nödvändig ändringen egentligen är. Frågan måste därför ställas om de generösare villkor för begagnande av hemliga tvångsmedel som infördes hösten 2004 var tillräckligt motiverade i själva lagstiftningsärendet, och detta särskilt mot bakgrund av att de nya villkoren innebar att rättssäkerhets- och integritetsskyddskrav övergavs som ditintills av lagstiftaren själv hade ansetts vara grundläggande.

Som skäl för att införa en straffvärdeventil anförde regeringen att den dåvarande ordningen hade vissa brister (prop. 2003/04:74 s. 32 f.). Som exempel nämndes tavelstölden på Moderna muséet hösten 1993, där förundersökningen avsåg brottet grov stöld. Trots att det enligt regeringen tämligen snart stod klart att de enskilda brottens straffvärde skulle överstiga två års fängelse, var det inte möjligt att använda hemlig telefonavlyssning eftersom brottet hade en straffskala där den nedre gränsen var sex månaders fängelse. Regeringen framhöll att det var ett viktigt samhällsintresse att med hjälp av effektiva tvångsmedel kunna utreda brott som i det enskilda fallet har ett mycket högt straffvärde, men som har en vid straffskala med lågt straffminimum. Det fanns därför ett behov av att i viss utsträckning kunna beakta straffvärdet för det enskilda brott som förundersökningen avser.

Beträffande förslaget att hemlig teleavlyssning och hemlig teleövervakning skulle kunna komma till användning även med avseende på en teleadress som den misstänkte ringer *till* eller på annat sätt kontaktar, anförde regeringen att de som begick brott i allt

större utsträckning använde sig av telefoner som inte kunde avlyssnas (a. prop. s. 38). Det hade således blivit allt svårare att nå de misstänkta genom hemlig teleavlyssning av deras egna teleadresser eller sådana adresser som de skulle kunna antas använda. Regeringen uttalade att vinsten för brottsbekämpningen uppvägde det intrång i enskildas integritet som kunde uppkomma vid avlyssning eller övervakning av en teleadress som den misstänkte kunde antas kontakta. För att ett sådant ingrepp i integritetsskyddet skulle kunna tillåtas, måste det dock enligt regeringen ställas särskilt höga krav på kopplingen mellan den misstänkte och teleadressen. Som förutsättning skulle därför gälla att det fanns synnerlig anledning att anta att den misstänkte skulle komma att ta kontakt med den teleadressen.

När det gällde undantaget från kravet på förekomsten av en skäligen misstänkt person vid hemlig kameraövervakning anförde regeringen att det fanns ett antal situationer där det av utredningsskäl vore angeläget att kunna använda hemlig kameraövervakning även när det inte finns någon som är skäligen misstänkt för ett sådant brott (a. prop. s. 41 f.). Som exempel på sådana situationer nämnde regeringen återkommande anlagda bränder i ett bostadsområde och upprepade försök till mord på vårdhem. Det var enligt regeringen självklart att skulle vara värdefullt från brottsutredningssynpunkt om tillstånd till hemlig kameraövervakning kunde beviljas i liknande fall. Regeringen ansåg därför att hemlig kameraövervakning i vissa fall skulle få användas trots att det inte fanns någon som var skäligen misstänkt för brottet. Som förutsättning skulle gälla att det var av synnerlig vikt för utredningen att övervakningen sker, ett krav som emellertid redan tidigare var gällande för all hemlig kameraövervakning.

Europakonventionens och regeringsformens krav på att en inskränkning i envars rätt till respekt för sitt privatliv etc. skall vara nödvändig torde som ett minimikrav innebära att man kan påvisa och beskriva ett *faktiskt* behov av en sådan inskränkning. Det är således inte tillräckligt att i allmänna ordalag resonera kring att det *kan* finnas ett behov av utvidgade möjligheter att använda ett tvångsmedel. När ett faktiskt behov väl är påvisat gäller det för lagstiftaren att väga detta behov mot vikten av att värna rättssäkerhet och personlig integritet, dvs. att göra en proportionalitetsbedömning. Det är därvid inte tillfyllest att lagstiftaren lakoniskt ”finner” att nyttan av ett på visst sätt utformat tvångsmedel är större än behovet av att bevara skyddet för den personliga integri-

teten på en intakt nivå, utan vad som krävs är en resonerande framställning där omständigheter som talar för tvångsmedlets supremati omsorgsfullt prövas och bryts mot de argument som talar i motsatt riktning. Utan en sådan noggrann genomgång saknas möjlighet till verklig insikt i vilka motiv som varit avgörande för lagstiftaren.

Om nödvändigheten av att införa ny integritetskränkande tvångsmedelslagstiftning inte förklaras på ett övertygande sätt finns risk att lagstiftningen möts med misstro och att medborgarnas förtroende för lagstiftningen och intentionerna bakom densamma minskar till skada för rättssamhället i stort.

Det ligger också i lagstiftarens eget intresse att ge en fyllig analys och beskrivning av motivbilden beträffande i princip all integritetsinskränkande lagstiftning. Om behovsanalysen är alltför knapphändig och ingen egentlig proportionalitetsavvägning görs löper lagstiftaren nämligen i värsta fall risken att de dömande instanserna med rätt eller fel underkänner lagstiftningen såsom stridande mot Europakonventionens och/eller regeringsformens krav i fråga om skyddet för den personliga integriteten.

Sett från dessa utgångspunkter kan en del invändningar riktas mot regeringens och riksdagens behandling av det lagstiftningsärende som hösten 2004 resulterade i ökade möjligheter till hemlig tvångsmedelsanvändning. Sålunda understöddes regeringens beskrivning av behovet av dessa ökade möjligheter inte av någon empiriskt baserad information, exempelvis i form av att brottsutvecklingen såg ut på ett visst sätt eller att förekomsten av icke avlyssningsbara telefoner hade gjort tvångsmedelsanvändningen mindre effektiv. Information av denna karaktär borde ha varit fullt möjlig att få fram med utnyttjande av polisens egen årliga rapportering över tvångsmedelsanvändningen. När det gällde införandet av den s.k. straffvärdeventilen, som innebar att hemliga tvångsmedel kunde tillgripas vid fler brottstyper än tidigare, exempelvis vid grov stöld, motiverades den strängt taget endast med att det var viktigt att effektivt kunna bekämpa sådana brott som tavelstölden på Moderna Muséet. Något nytt eller tidigare oförutsebart motiv för en mer liberal tvångsmedelsanvändning var det knappast fråga om, däremot om en annan värdering av balansen mellan brottsbekämpning och integritet. Skälen för denna nya värdering redovisas emellertid inte annat än i ytterst allmänna och svepande ordalag. De djupare övervägandena som legat till grund för rubbandet av balansen mellan dessa båda intressen kan den utomstående betraktaren endast gissa sig till.

Flera år innan reformen genomfördes hade Lagrådet yttrat sig över förslag som i mycket liknade de som kom att genomföras. Lagrådet hade då nöjt sig med att i huvudsak hänvisa till att åtskilliga av de – kritiska – synpunkter som Lagrådet hade fört fram beträffande lagförslag om buggning hade bäring också på förslagen till de här aktuella tvångsmedlen. I fråga om den s.k. straffvärdeventilen hade Lagrådet emellertid särskilt anmärkt att denna framstod som tvivelaktig eftersom den innebar att hemlig teleövervakning kan användas som tvångsmedel vid många brott som kan leda till en icke frihetsberövande påföljd.

Utvidgade möjligheter att ta DNA-prov

Genom lagändringar som trädde i kraft den 1 januari 2006 infördes möjlighet att ta DNA-prov enbart i syfte att uppgifter från DNA-analysen skall kunna föras in i det nyinrättade utredningsregistret. Eftersom denna nya möjlighet att ta DNA-prov sålunda har ett nära samband med inrättandet av utredningsregistret, lämnas en samlad kommentar till dessa lagändringar i avsnitt 11.3.4. I detta sammanhang kan dock påpekas att den tidigare svenska regleringen om tagande av DNA-prov hade utformats i enlighet med Europarådets rekommendation No. R (92) om användning av DNA-analys inom ramen för det straffrättsliga systemet. Den nya möjligheten att ta DNA-prov samt att registrera uppgifter från analysen enbart för framtida behov avviker i flera avseenden från Europarådets rekommendation.

I samband med lagstiftningsärendet om utvidgade möjligheter att använda DNA-teknik i brottsbekämpningen påpekade Lagrådet att frågan om verkan av den enskildes samtycke borde tas upp till principiellt övervägande i detta sammanhang, eftersom prov för DNA-analys i så stor utsträckning har tagits och förutses komma att tas efter samtycke av den enskilde. Särskilt som frågan rör begränsning av en grundlagsskyddad rättighet talade enligt Lagrådet starka skäl för att rättsläget klargörs genom uttrycklig lagreglering.

Beträffande husrannsakan föreskrivs i 28 kap. 1 § tredje stycket RB att för husrannsakan hos den misstänkte inte i något fall får åberopas hans samtycke, om han inte själv begärt åtgärden. Någon motsvarande reglering av verkan av samtycke finns inte i fråga om kroppsvisitation och kroppsbesiktning. I förordningen (1992:824)

om fingeravtryck m.m. finns i 2 § en bestämmelse som medger att fingeravtryck får tas av den som inte är misstänkt för brott, om det behövs för att utreda det aktuella brottet och fängelse kan följa på detta.

JO har uttalat (2003/04 :JO1 s. 75 f.) att det är i viss mån oklart hur långt grundlagsskyddet sträcker sig när det gäller kroppsbesiktning, eftersom skyddet endast avser påtvingade kroppsliga ingrepp. Enligt JO står det emellertid i bäst överensstämmelse med rättssäkerhetens krav att grundlagsregeln tolkas så, att den ställer upp ett skydd också mot att en befattningshavare vid en brottsutredande myndighet – utan att använda eller vara beredd att använda tvång i egentlig bemärkelse – uppträder på ett sätt som får till följd att någon med fog uppfattar sig vara tvungen att underkasta sig exempelvis en undersökning eller provtagning. JO framhöll att det är tydligt att det finns en särskilt stor risk för att situationer av nu nämnt slag skall uppkomma, när åtgärden avser en person som har klart för sig att han inte är fri från misstanke om det brott som utredningen avser.

Kommittén instämmer i JO:s bedömning att den oklarhet som föreligger vad gäller den rättsliga betydelsen av att någon, som visserligen kan misstänkas för brott men inte är skäligen misstänkt, samtycker till att underkasta sig åtgärder av det slag som avses med bestämmelsen om kroppsbesiktning är i hög grad otillfredsställande. Det finns en uppenbar risk för att frivilligheten i en sådan situation blir närmast illusorisk. Därmed är det svårt för den ansvarige befattningshavaren att avgöra om samtycket verkligen lämnas frivilligt eller om det blir fråga om en otillåten kroppsbesiktning. Som JO påpekat blir det än svårare för en utomstående granskare att i efterhand bedöma om medverkan i en brottsutredning var resultatet av otillbörliga påtryckningar eller ej. Den omständigheten att det nu införts möjlighet att tvångsvis ta DNA-prov också från annan än den misstänkte gör det än mer angeläget att rättsläget beträffande verkan av den enskildes samtycke klargörs genom en uttrycklig lagreglering.

9.5.4 Pågående reformarbete om buggning och preventiv användning av hemliga tvångsmedel

Preventiv användning av hemliga tvångsmedel

Det i riksdagen nu vilande förslaget om en ny lag som tillåter att hemliga tvångsmedel används i förebyggande syfte får anses mycket ingripande från integritetssynpunkt och ha stor principiell betydelse. Innebörden av den nya lagen är att avsteg görs från det krav som ansetts vara det kanske mest grundläggande vid all hemlig tvångsmedelsanvändning, nämligen att tvångsmedel enbart får användas under förundersökning av ett brott. Användning av tvångsmedel har de facto hitintills alltid inneburit just att en förundersökning har inletts. Med den nya lagen blir alltså tvångsmedelsanvändning tillåten *innan* ett brott överhuvudtaget har begåtts och skall därmed avse personer som *kan* komma att begå brott.

Enligt gällande ordning är användning av tvångsmedel i förebyggande och förhindrande syfte visserligen tillåten med stöd av bestämmelserna i lagen (1991:572) om utlänningskontroll. Det handlar emellertid då om det mycket speciella fallet att en utlänning befaras komma att begå eller medverka till terroristbrott. Den nya lagen innebär att användning i preventivt syfte kan komma till användning i betydligt större utsträckning inom Säkerhetspolisens verksamhet, men också inom den verksamhet som bedrivs av den öppna polisen när det är fråga om bekämpande av systemhotande brottslighet.

Förutom att lagen innebär avsteg från det annars grundläggande kravet att tvångsmedel endast får användas under förundersökning av ett brott, innebär det också i ett annat avseende avsteg från de krav som i dag gäller för tvångsmedelsanvändning under förundersökning. Sålunda skall det inom ramen för postkontroll vara möjligt att undersöka, öppna och granska brev och andra försändelser utan att beslag av försändelsen sker och utan att avsändaren, mottagaren eller någon annan underrättas om åtgärden (jfr 27 kap. 9–12 § RB).

Varken Europakonventionen eller regeringsformen uppställer något förbud mot att tvångsmedel används i förebyggande syfte. De tvångsmedel som omfattas av den nya lagen innebär emellertid väsentliga intrång i enskilda människors rätt till respekt för sitt privatliv och sin korrespondens. För att deras användning skall

kunna godtas måste det föreligga ett så starkt behov att det är proportionerligt i förhållande till inskränkningarna i integritetsskyddet, och tillämpningsområdet får inte heller bli större än vad som är nödvändigt för att tillgodose behovet (jfr Lagrådet, prop. 2005/06:177 s. 114).

I proposition 2005/06:177 lämnas en viss redovisning av Säkerhetspolisens respektive den öppna polisens behov av att använda de aktuella tvångsmedlen i förebyggande syfte. En mer utförlig redovisning av detta behov lämnas i departementspromemorian *Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet* (Ds 2005:21) som tjänat som underlag för propositionen. Behovet av att använda tvångsmedel för att förebygga den typ av brottslighet som omfattas av lagen kan sålunda anses godtagbart redovisat. Någon egentlig analys av vilka konsekvenser för integritetsskyddet som denna typ av tvångsmedelsanvändning kan komma att medföra redovisades däremot inte. Därmed har det inte heller varit möjligt att göra den proportionalitetsbedömning som är en förutsättning enligt såväl regeringsformen som Europakonventionen vid införandet av rättighetsinskränkande lagstiftning. I sin redovisning av förslagens betydelse för integritetsskyddet och hur detta skulle vägas mot behovet och effektiviteten av den föreslagna användningen av tvångsmedel nöjde sig regeringen med att konstatera att medborgarnas berättigade krav på trygghet och skydd mot terrorism och annan samhällsfarlig brottslighet vägde tyngre än de presumtiva gärningsmännens intresse av skydd mot övervakning och kontroll. Regeringen påpekade vidare att användningen av hemliga tvångsmedel i och för sig kan inkräkta på tredje mans integritetsintressen. De behovs- och effektivitetsskäl på det brottsförebyggande området som talar för förslaget vägde emellertid så tungt att tredje mans integritetsintressen i viss mån fick stå tillbaka i dessa fall. Någon närmare analys av konsekvenserna för den enskildes integritet lämnades dock inte.

För att efterkomma Lagrådets synpunkter på att frågan huruvida rätten enligt artikel 13 i Europakonventionen till ett effektivt rättsmedel var tillgodosedd inte alls hade berörts i lagrådsremissen, aviserade regeringen att den avsåg att tillsätta en utredning med uppgift att skyndsamt lämna förslag på lagstiftning om underrättelseskyldighet vid användning av tvångsmedel. Denna utredning har nyligen i betänkandet *Ytterligare rättssäkerhet vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98) föreslagit att det skall införas en särskild skyldighet att underrätta enskilda personer som

har berörts av användning av hemliga tvångsmedel. Om utredningens förslag genomförs kommer detta otvivelaktigt att innebära en förstärkning av integritetsskyddet på tvångsmedelsområdet. Oavsett detta synes underlaget för lagförslaget behöva kompletteras för att det skall bli möjligt att göra en sådan proportionalitetsbedömning som enligt såväl regeringsformen som Europakonventionen utgör en förutsättning för rättighetsbegränsande lagstiftning.

Det bör i detta sammanhang påpekas att den nya lagen om användning av hemliga tvångsmedel i förebyggande syfte har för Säkerhetspolisens del ansetts kunna rätta till det problem som i dag anses föreligga genom att gällande ordning ger uttryck för dubbla budskap från statsmakternas sida. Tvångsmedelsanvändningen kan härigenom ske på ett sätt som bättre stämmer överens med Säkerhetspolisens uppgift att uppdaga och förhindra brottslig verksamhet och en extensiv tolkning av tvångsmedelsreglerna behöver inte längre tillämpas. Denna fråga berörs ytterligare i kapitel 12.

Buggning

Det förslag till en ny lag om hemlig rumsavlyssning, härefter benämnt buggning, som för närvarande vilar i riksdagen, tillåter en användning av tvångsmedel som är synnerligen integritetskänslig. Buggning får anses avsevärt mer ingripande i den enskildes integritet än hemlig teleavlyssning, som i sig anses som mycket integritetskränkande. Som JO anförde vid remissbehandlingen får det snarare ses som en artskillnad än en gradskillnad av ingreppet i den enskildes integritet. Användning av buggning innebär att det tillåts att polisen med våld bereder sig tillträde till en misstänkt persons hem och där installerar en teknisk anordning som medger att de samtal som förs i bostaden och andra ljud kan avlyssnas. Medan hemlig teleavlyssning är begränsat till att avse den del av en persons dagliga aktiviteter som utgörs av telefonsamtal och annan elektronisk kommunikation, kan buggning avse vilken plats som helst, omfatta hela dygnet och registrera varje samtal och andra ljud. När avlyssningen har avbrutits får polisen på nytt bryta sig in för att avlägsna den tekniska anordningen. Enligt lagen tillåts buggning också av bostad som tillhör annan än den misstänkte.

Som Lagrådet påpekat både i samband med 2000 års lagrådsremiss och vid beredningen av det nu aktuella lagförslaget, måste

det för att ett så ingripande tvångsmedel som buggning skall få införas krävas mycket starka skäl. Lagrådet avstyrkte vid båda tillfällena att en lagstiftning som tillåter buggning införs. Vid det första tillfället ansåg Lagrådet att behovet inte hade visats tillräckligt reellt och starkt, att det fanns svagheter i den föreslagna systemet med offentliga ombud samt att en utförlig reglering för behandling av överskottsinformation saknades. I samband med det nu aktuella lagförslaget ansåg Lagrådet att behovet av en lag om buggning med ett så vidsträckt tillämpningsområde som föreslogs inte kunde anses framgå av de upplysningar om behovet som lämnats. Det kunde också ifrågasättas om det föreslagna systemet fyller rimliga krav på rättssäkerhet och överensstämmer med Europakonventionen.

När det gäller Säkerhetspolisens verksamhet är det allmänt känt att terrorism har utvecklats till ett stort problem som också drabbat vårt lands närområden. Beträffande Säkerhetspolisens verksamhet i övrigt vad avser kontraspionage och författningsskyddande verksamhet kan propositionen knappast anses ge belägg för att behovet av buggning har ökat under senare år. De exempel som lämnades visar också på svårigheten att göra den gränsdragning som fordras mellan användning av buggning för utredning av ett begånget brott och som spaningshjälpmedel, vilket inte skall vara tillåtet. I fråga om den öppna polisens verksamhet gavs en viss redovisning av behovet av buggning för att utreda en ökande organiserad och systemhotande brottslighet. En mer utförlig redovisning av sådan brottslighets utveckling lämnades i departementspromemorian Ds 2005:21. Någon redovisning av behovet för utredning av de övriga brottstyper där buggning skall vara tillåten lämnades inte alls. Regeringen anförde därvid endast att buggning borde kunna användas vid förundersökning även angående andra särskilt grova brott i de enstaka fall då utredningen inte kunde föras framåt på annat sätt.

Beträffande frågan om buggning kan anses vara en effektiv metod i samband med utredning av brott hänvisade regeringen till samtal som man har haft med företrädare för polismyndigheter i vissa länder samt till undersökningar som gjorts i Tyskland och Finland. Undersökningen i Finlad omfattade inte avlyssning av bostäder. Enligt dessa undersökningar synes buggning i de båda länderna ha varit en mindre effektiv metod än vad hemlig teleavlyssning är i Sverige. Det torde kunna sättas i fråga om den lämnade redovisningen utgör ett tillräckligt underlag för att bedöma

buggningens effektivitet i samband med brottsutredning i vårt land och med de möjligheter till annan tvångsmedelsanvändning som finns här.

Någon närmare analys av vilka konsekvenser användningen av buggning kan få för integritetsskyddet redovisades inte i propositionen. Regeringen konstaterade endast att behovet av buggning och dess effektivitet i den brottsutredande verksamheten väger så tungt och innebär sådana vinster för det allmänna att en inskränkning i rättigheterna enligt 2 kap. 6 § RF och artikel 8 i Europakonventionen är godtagbar.

Sammanfattningsvis kan sägas att det krävs mycket starka skäl för att ett så synnerligen ingripande tvångsmedel som buggning skall få tillåtas. Den behovsredovisning som finns tillgänglig i lagstiftningsärendet täcker bara delvis det föreslagna tillämpningsområdet. Någon närmare analys av konsekvenserna för integritetsskyddet har inte lämnats. Underlaget synes därför behöva kompletteras för att det skall bli möjligt att göra en sådan proportionalitetsbedömning som enligt såväl regeringsformen som Europakonventionen utgör en förutsättning för rättighetsbegränsade lagstiftning.

9.5.5 Kommentar till kontrollen av tvångsmedlens användning

Den parlamentariska kontrollen

Den parlamentariska kontrollen av de hemliga tvångsmedlen, som baseras på regeringens årliga skrivelse till riksdagen om hur reglerna om de hemliga tvångsmedlen har tillämpats, bör ses i ljuset av bland annat de uttalanden som Europadomstolens har gjort om att det måste finnas en effektiv kontroll av att tvångsmedelssystemet inte missbrukas.

Som framgått har det varit en återkommande fråga hur redovisningen för den parlamentariska kontrollen kan förbättras. På senare tid har denna fråga framför allt gällt redovisningen av *andelen* fall där tvångsmedlet ”har haft betydelse för förundersökningen beträffande den misstänkte”. Redovisningen har i denna del ansetts svårbedömd. Någon närmare uppmärksamhet synes däremot inte ha ägnats frågan om hur hög denna andel bör vara för att respektive tvångsmedelsanvändning skall kunna anses fungera effektivt. En tänkbar förklaring till att denna fråga inte uppmärksammats skulle

kunna vara att det inte ansetts lönt att närmare fundera över frågan så länge som själva bedömningsunderlaget är svårtydbart.

Andelen tillstånd till användning av hemliga tvångsmedel som ”har haft betydelse för förundersökningen beträffande den misstänkte” har för det mesta understigit 50 procent av antalet meddelade tillstånd. Den lägsta andelen fall som uppfyllt detta kriterium uppvisar hemlig kameraövervakning. Motsvarande andelstal för hemlig teleavlyssning och hemlig teleövervakning har under senare år legat på mellan 40 och 50 procent.

I Åklagarmyndighetens och Rikspolisstyrelsens redovisning till Justitiedepartementet har det, utöver uppgifterna i vad mån förundersökningen har haft betydelse, förts in bedömningsgrunden ”Polisingripande/fört undersökningen framåt”. Det finns emellertid ingen redovisning av andelen tillstånd som t.ex. lett till fällande dom. Sådan redovisning finns endast för antalet förundersökningar (i vilken kan ingå flera misstänkta, medan tillstånd till tvångsmedel lämnas för varje individ för sig).

Att andelen tillstånd som ”har haft betydelse för förundersökningen beträffande den misstänkte” inte är högre skulle kunna uppfattas som att tvångsmedelsanvändningen inte är särskilt effektiv. Frågan är dock vad den förväntade effektiviteten egentligen är. En annan relevant fråga är vad som allmänt sett är en rimlig grad av effektivitet. Nyckelord i sammanhanget torde vara kravet på att tvångsmedlet skall vara av ”synnerlig vikt” för utredningen.

I förarbetena anfördes att uttrycket synnerlig vikt inte nödvändigtvis är detsamma som att avlyssningen skall ge avgörande bevisning som omedelbart kan leda till fällande dom (prop. 1988/89:124 s. 44 f.). Däremot inrymde enligt föredragande statsrådet uttrycket synnerlig vikt ett kvalitetskrav beträffande de upplysningar som avlyssningen kunde ge. Dessa fick sålunda inte inskränka sig till obetydliga detaljer, som man både kunde ha och mista. Uttrycket innefattade därutöver ett krav på att utredningsläget gjorde avlyssningen nödvändig. Vad som kunde vinnas med åtgärden fick i princip inte vara åtkomlig med andra, mindre ingripande metoder. Någon slentrianmässig bedömning fick inte förekomma, utan en granskning av utredningsmöjligheterna i det enskilda fallet måste alltid verkställas. Enligt föredragande statsrådet behövde det inte föreligga något absolut hinder mot att få fram information på andra vägar. Det krävdes dock att hindret är sådant att det inte skäligen kan begäras att man skall avstå från teleavlyssningen. Statsrådet nämnde som exempel härpå orimligt hög

personalinsats eller avsevärd risk för att den pågående utredningen skulle avslöjas för tidigt.

Den s.k. Edenmankommissionen, vars ena rapport (SOU 1988:18) låg till grund för proposition 1988/89:124 tillsammans med bl.a. betänkandena från Tvångsmedelskommittén, menade att vad som kommer fram vid telefonavlyssning sällan är av sådan beskaffenhet att det kan användas som bevis i rättegång. Däremot kunde materialet främja spaningen genom att ge en inblick i den misstänktes miljö. När det gällde att bedöma om telefonavlyssning var av synnerlig vikt för utredningen borde därför enligt kommissionen anspråken på den bevismässiga betydelsen av förväntade informationer inte sättas särskilt högt. Den begränsning som var påkallad av integritetsskäl låg huvudsakligen däri att brottet skulle vara av viss angiven svårhetsgrad.

Av förarbetena torde alltså kunna utläsas åtminstone att andelen tillstånd som lett till fällande dom inte ansetts ha någon avgörande betydelse för huruvida tvångsmedelsanvändningen skall anses effektiv. Frågan kvarstår dock vad den förväntade effektiviteten egentligen är. Svaret på denna fråga bör ju vara av betydelse inte bara vid tillståndsgivningen, då det skall avgöras om tvångsmedlet är av synnerlig vikt för utredningen, utan också för den parlamentariska kontrollen. Om man inte vet vad den förväntade effektiviteten är, saknar man grund för att alls bedöma om ett tvångsmedel är effektivt. Man kan heller inte bedöma om t.ex. en ökning av antalet meddelade tillstånd, samtidigt som effektiviteten minskar, är ett tecken på att tillstånd medges alltför slentrianmässigt. Vad man förväntar sig i form av effektivitet får betydelse också för redovisningens innehåll. Någon anledning att redovisa poster som det inte går att göra någon bedömning av finns naturligtvis inte, medan däremot i princip alla poster som bidrar till att ge en rättvisande bild bör redovisas.

Det kan alltså konstateras att det inte finns någon stadgad uppfattning om vad den förväntade effektiviteten – i relation till uttrycket ”synnerlig vikt” – av tvångsmedelsanvändning är eller bör vara. Därmed inskränks den parlamentariska kontrollen över tvångsmedlens effektivitet till enbart jämförelser mellan andelen resultatrika tvångsmedelsanvändningar från ett år till ett annat. Detta förhållande är knappast tillfredsställande från integritetsskyddssynpunkt.

Den årliga redovisningen till riksdagen baseras i stort sett enbart på uppgifter från Åklagarmyndigheten och Rikspolisstyrelsen.

Dessa uppgifter ställs inte i relation till andra uppgifter som kan vara relevanta i sammanhanget, t.ex. BRÅ:s statistik över antalet personer misstänkta för brott och över brott som lett till att personer lagförts (detta skedde dock vid enstaka tillfällen under 1980-talet). En kompletterande uppgift som numera lämnas rör beslag av narkotika. Variationer i antalet sådana beslag kan antas ha relevans för narkotikabrottslighetens utveckling i stort. Uppgiften har dock inte någon omedelbar relevans för en värdering av tvångsmedelsanvändningen, eftersom uppgiften inte säger något om vare sig antalet begångna grova narkotikabrott eller antalet personer misstänkta för sådant brott.

Av BRÅ:s statistik framgår vidare att antalet lagföringar för grova narkotikabrott har legat relativt konstant under den senaste tioårsperioden (däremot har en kraftig ökning skett av de ringa brotten avseende eget bruk och mindre innehav). Smugglingen uppvisade en kraftig nedgång från år 1993 till 2000, vilken kunde förklaras med tullens förändrade rutiner i samband med EU-inträdet. Under senare år har man närmat sig samma nivå som tidigare (EU-inträdet och Schengensamarbetet anses dock göra statistiken svår att tolka).

Antalet meddelade tillstånd till hemlig teleavlyssning och hemlig teleövervakning har ökat kraftigt under senare år, men har således inte någon motsvarighet i statistiken över antalet lagföringar för grova narkotikabrott. Som förklaring till ökningen av antalet meddelade tillstånd har regeringen anfört att polisen har fått bättre tekniska möjligheter till avlyssning och kan avlyssna nya typer av telefoner. Det har också framförts att ett stort antal tillstånd kunde meddelas inom ramen för samma förundersökning, eftersom flera personer ofta (underförstått oftare än tidigare) är inblandade i samma kriminella verksamhet. Uppenbarligen är det dock svårt för att inte säga omöjligt att enbart utifrån de lämnade uppgifterna kontrollera i vad mån det finns andra förklaringar till den kraftiga ökningen av antalet tillstånd.

Åtskilliga anmärkningar av systemkaraktär kan alltså riktas mot det sätt varpå den parlamentariska kontrollen över tvångsmedelsanvändningen bedrivs. Årsvisa fluktuationer i antalet meddelade tillstånd och i andelen resultatrika fall kommenteras inte närmare, och bakgrundsmaterial och jämförande material redovisas inte. Exempelvis redovisas beslag av narkotika men inte statistik över antalet personer misstänkta, åtalade och dömda för narkotikabrott. Ingen förklaring till eller analys av orsakerna har givits till att den

redovisade statistiken över tvångsmedelsanvändningen ser ut som den gör. Några andra uppgifter än sådana som härrör från Åklagarmyndigheten och Rikspolisstyrelsen synes inte beaktas inom ramen för den parlamentariska kontrollen.

Sammantaget torde det kunna ifrågasättas om den parlamentariska kontrollen över användningen av de hemliga tvångsmedlen för närvarande bedrivs effektivt. Säkert är i varje fall att det finns utrymme för förbättringar av denna kontroll.

Offentliga ombud

Även den nyligen införda ordningen med offentligt ombud i ärenden om användning av hemlig teleavlyssning och hemlig kameraövervakning bör ses mot bakgrund av att Europadomstolen slagit fast att det i konventionsstaterna måste finnas en effektiv kontroll av att tvångsmedelssystemet inte missbrukas. Om syftet med de offentliga ombuden är att kompensera den ökade risk för integritetsförluster som reformeringen av tvångsmedelsanvändningen hösten 2004 innebar, är det naturligtvis väsentligt att ett system samtidigt införs som gör det möjligt att effektivt kontrollera hur väl ordningen med offentliga ombud fyller detta syfte.

I betänkandet SOU 2006:98 har en översyn av systemet med offentliga ombud gjorts. Utredaren bedömer att systemet fungerar väl och föreslår inga ändringar i gällande ordning. Dennes bedömning synes baseras främst på muntliga uppgifter som lämnats vid ett samrådsmöte.

Varken Regeringskansliet eller den ovan nämnda utredningen, som har haft mycket kort tid på sig för sitt arbete, har inhämtat faktiska uppgifter om i vilken utsträckning de offentliga ombuden har överklagat besluten om användning av tvångsmedel. Det finns heller ingen faktisk uppgift om i vilken utsträckning ärenden har ansetts så brådskande att något ombud inte har förordnats. Ett sådan uppföljning av ordningen med offentliga ombud borde genomföras för att ge ett mer tillfredsställande underlag för hur systemet fungerar.

9.5.6 Internationella överenskommelser om rättslig hjälp

Någon anledning att på förhand utgå från att andra länders regler för tvångsmedelsanvändning ger ett sämre integritetsskydd än de svenska reglerna finns givetvis inte. Rent faktiskt kan det emellertid konstateras att den inom EU alltmer vanliga ordningen med ömsesidigt erkännande i vissa fall får till effekt att rent nationella skyddsregler, på olika normgivningsnivåer, genombryts och sätts ur spel. En motverkande faktor i det sammanhang är att alla EU:s medlemsstater är bundna av Europakonventions krav och därmed förpliktade att ha en lagstiftning som tillgodoser konventionsbestämmelserna om respekten för den enskildes privatliv etc. Det är i själva verket detta förhållande som har utgjort grunden för det EU-rättsliga systemet med ömsesidigt erkännande.

10 Polisens spaningsmetoder

Huvudsaklig bedömning:

– Med hänsyn till skyddet för den enskildes integritet bör det införas en mer uttrycklig reglering av polisens integritetskänsliga spaningsmetoder än vad som finns i dag.

10.1 En förstärkt brottsförebyggande verksamhet

Enligt ett äldre synsätt skulle polisens brottsbekämpande verksamhet väsentligen vara reaktivt inriktad. Utgångspunkten kan sägas ha varit att polisen skulle ägna sig åt att utreda misstankar om konkreta brott och att personer som inte var misstänkta för konkreta brott skulle lämnas i fred. För att förstärka och utveckla det brottsförebyggande arbetet presenterade regeringen år 1996 *Allas vårt ansvar – ett nationellt brottsförebyggande program* (Ds 1996:59). Med detta som utgångspunkt och med beaktande av erfarenheterna sedan dess anser regeringen att det brottsförebyggande arbetet numera skall utgå från följande perspektiv (prop. 2005/06:1, utgiftsområde 4 s. 26 f.):

> Det brottsförebyggande arbetet är allas ansvar. Det skall vara en integrerad del av övriga politikområden. Det krävs samverkan och närvaro på alla nivåer. Arbetet skall bygga på kunskap och ha ett långsiktigt perspektiv. - - - Polisen är en nyckelaktör i det brottsförebyggande arbetet genom sin specialkompetens i fråga om brott som samhällsföreteelse och sin kunskap om praktiska brottsförebyggande åtgärder. Genom sin samverkan med en rad aktörer har polisen en central position i samhällets brottsförebyggande arbete.

Polisdatautredningen framhåller i sitt betänkande *Behandling av personuppgifter i polisens verksamhet* (SOU 2001:92 s. 113 f.) att polisen, för att kunna verka brottsförebyggande, måste inhämta

och bearbeta information i större utsträckning än som sker vid ett traditionellt reaktivt arbetssätt. Denna verksamhet kan inte enbart ske inom ramen för förundersökningar. För ett framgångsrikt arbete är det nödvändigt att samla in och bearbeta även underrättelser som innehåller personuppgifter. Underrättelseverksamheten bedrivs på alla nivåer inom polisväsendet, inte minst i det vardagliga polisarbetet ute på fältet. Genom egna iakttagelser, tips eller upplysningar samlar polisen fortlöpande in sådan information som ger anledning att misstänka att brottslig verksamhet förekommer. Utredningen påpekar att en insamling och bearbetning av personuppgifter av här skisserat slag innebär att polisen inte enbart kan behandla uppgifter om personer som är misstänkta för konkreta brott. För att behandlingen av personuppgifter skall kunna fylla sitt syfte måste insamlingen av personuppgifter ske tidigare. Behandlingen behöver innefatta uppgifter om misstankar mot enskilda personer redan vid en låg grad av misstanke. Ibland är det nödvändigt att samla in uppgifter om misstankar mot enskilda personer, även om misstankarna inte kunnat preciseras till att avse en viss specifik händelse eller gärning. Utredningen framhåller att det således ligger i sakens natur att en brottsförebyggande arbetsmetod innebär ett ökat intrång i den enskildes personliga integritet i förhållande till ett reaktivt arbetssätt. Detta skall vägas mot effektiviteten i brottsbekämpningen.

10.2 Kort om regelverket

10.2.1 Allmänt om polisens rätt att samla information

Varken i rättegångsbalken eller i någon annan lagstiftning finns några allmänna regler om polisens rätt att inhämta information. Däremot finns bestämmelser som i vissa särskilda fall reglerar en sådan rätt. Som exempel kan nämnas bestämmelserna om de straffprocessuella tvångsmedlen i 27 och 28 kap. RB. Dessa bestämmelser är begränsade till inhämtande av information under förundersökning. En reglering av polisens rätt att inhämta information med hjälp av dessa tvångsmedel har ansetts nödvändig på grund av att åtgärden i fråga annars skulle strida mot 2 kap. 6 § RF eller mot bestämmelser i brottsbalken. Någon allmän bestämmelse om polisens rätt att skaffa information från andra myndigheter finns inte heller. I sådana fall är polisen i första hand hänvisad till de förfaran-

den som anvisas i 14 kap. och 15 kap. SekrL för myndigheters utbyte av information. Det förekommer också att polisen använder sig av tvångsmedlen husrannsakan eller beslag för att få tillgång till information från andra myndigheter.

10.2.2 Polislagens 8 §

Under det spaningsskede som föregår en förundersökning är rättegångsbalkens bestämmelser om tvångsmedel inte tillämpliga. Några andra regler som uttryckligen reglerar polisens rätt att inhämta information i denna del av polisarbetet finns inte heller. Däremot finns en bestämmelse i polislagen (1984:387) – 8 § – som anger de allmänna grundsatser som skall iakttas för att ett ingripande från polisens sida skall vara godtagbart.

En polisman som har att verkställa en tjänsteuppgift skall enligt 8 § första stycket polislagen under iakttagande av vad som föreskrivs i lag eller annan författning ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Måste tvång tillgripas, skall detta ske endast i den form och den utsträckning som behövs för att det avsedda resultatet skall uppnås.

I 8 § andra stycket föreskrivs att ett ingripande som begränsar någon av de grundläggande fri- och rättigheter som avses i 2 kap. RF inte får grundas enbart på bestämmelserna i första stycket.

De principer som anges i 8 § polislagen har generell betydelse för polisarbetet. Principerna får bl.a. betydelse när polisen skall ta ställning till val av spaningsmetoder. Paragrafen kan ses som ett allmänt bemyndigande för polisen att vidta de åtgärder som är försvarliga för att fullgöra dess uppgifter, så länge det inte är fråga om att begränsa en grundlagsskyddad rättighet eller att vidta åtgärder som står i strid mot någon specialreglering.

En närmare redovisning av den befintliga regleringen på området – 8 § polislagen – lämnas i kapitel 29. Där redovisas också vissa avgöranden från Europadomstolen samt beslut från JO och JK som rört användningen av tekniska spaningsmetoder.

10.3 Vissa integritetskänsliga spaningsmetoder

10.3.1 Vilka metoder har diskuterats från ett integritetsskyddsperspektiv?

Frånvaron av uttryckliga regler för polisens rätt att genom olika metoder inhämta information har framför allt kommit att diskuteras när det gäller polisens användning av en typ av arbetsmetoder som något diffust brukar benämnas okonventionella spaningsmetoder. Sådana spaningsmetoder kan även användas under en förundersökning, men det är vanligare att metoderna används under spaningsskedet. Dessa spaningsmetoder utgörs främst av olika typer av provokation och infiltration samt av metoder som kräver att tekniska hjälpmedel används. Metoderna har diskuterats ända sedan 1970-talet, då Rikspolisstyrelsen inledde ett utvecklingsarbete när det gällde bl.a. metoder vid spaning mot ekonomisk brottslighet och grov narkotikabrottslighet. De frågor som har diskuterats har framför allt gällt vilka metoder som från rättssäkerhets- och integritetssynpunkt bör kunna tillåtas samt i vilken utsträckning det är lämpligt eller t.o.m. nödvändigt att utforma rättsregler som ger ett utryckligt lagstöd för metoderna.

De spaningsmetoder som utgör olika typer av provokation och infiltration, och där polisen genom någon form av vilseledande eller manipulation inhämtar information, väcker frågor som inte i första hand rör den personliga integriteten utan som framför allt är av intresse från rättssäkerhetssynpunkt. Dessa metoder har därför inte något omedelbar relevans för kommitténs arbete och kommer inte att behandlas här. I detta sammanhang kan dock nämnas att en ny lag om kvalificerade skyddsidentiteter för tjänstemän inom polisen och Försvarsmaktens försvarsunderrättelseverksamhet trädde i kraft den 1 oktober 2006 (prop. 2005/06:149, bet. 2005/06:JuU31). Lagen reglerar inte rätten att använda kvalificerad skyddsidentitet, eftersom detta inte ansetts behövas vare sig med hänsyn till legalitetsprincipen eller till rättssäkerhets- eller effektivitetsintressen, utan reglerna anger förutsättningarna och formerna för skapandet av en kvalificerad skyddsidentitet.

Spaningsmetoder som innebär att tekniska hjälpmedel används för att inhämta information ger däremot i allmänhet upphov till frågor från integritetssynpunkt, eftersom de tar sikte på avlyssning eller övervakning i någon form. Nedan lämnas en kort redogörelse

för spaningsmetoder av denna typ, som härefter benämns *tekniska spaningsmetoder.*

10.3.2 Vissa tekniska spaningsmetoder

Uppgifterna nedan är framför allt baserade på betänkandet *Ökad effektivitet och rättssäkerhet i brottsbekämpningen* (SOU 2003:74 s. 75–94) samt på kompletterande muntlig information lämnad av företrädare för Rikskriminalpolisens spaningsrotel under november 2005.

Handmanövrerade kameror

Det finns olika sätt att inhämta information genom kameraövervakning. Övervakning kan för det första ske genom användning av fjärrmanövrerade kameror. Sådan övervakning är redan lagreglerad genom dels lagen (1998:150) om allmän kameraövervakning, dels lagen (1995:1506) om hemlig kameraövervakning. En annan metod för kameraövervakning är att använda handmanövrerade kameror. Denna metod är inte lagreglerad. Den lagstiftning som reglerar behandling av personuppgifter begränsar dock i viss utsträckning den praktiska användningen av digitala kameror. Det kan också nämnas att det i 28 kap. 14 § RB finns bestämmelser om att den som är anhållen eller häktad bl.a. kan fotograferas. Närmare bestämmelser finns i förordningen (1992:824) om fingeravtryck m.m. Av denna förordning framgår att regleringen numera också omfattar videofilmning med handmanövrerad kamera. Även annan person än den som är anhållen eller häktad får filmas på det sättet, om det behövs för att utreda ett brott på vilket det kan följa fängelse (jfr JO 1999/2000 s. 91).

Det är mycket vanligt att polisen använder sig av videofilmning med handmanövrerade kameror. Oftast filmas enskilda misstänkta och personer som dessa träffar. Även filmning in i eller strax utanför bostäder förekommer. Vanligast är dock att filmningen äger rum i offentliga miljöer. Det förekommer också användning av stillbildskamera. Beslut om att använda handmanövrerade videokameror fattas av den enskilde polismannen och någon särskild dokumentation över användningen görs inte.

Beredningen för rättsväsendets utveckling har påpekat att det med dagens teknik är möjligt att på distans styra kameror, även om det fortfarande är en enskild polisman som styr kameran (a. bet. s. 76). I framtiden kan det därför uppstå situationer där gränsen mellan vad som skall anses vara fjärrmanövrerade kameror och handmanövrerade kameror blir otydlig. I den mån den nya tekniken med distansstyrda kameror används av polisen i dag, sker detta först efter att tillstånd för hemlig kameraövervakning har meddelats.

Dolda kroppsmikrofoner

Dold kroppsmikrofon används för att i hemlighet avlyssna ett samtal, genom att samtalet spelas in eller genom att någon utomstående direkt tillåts ta del av samtalet. Mikrofonutrustningen fästs på polismannens kläder eller direkt på kroppen. Det förekommer också att utrustningen bärs av en annan person som polisen samarbetar med. Dold mikrofon behöver inte fästas på kläderna utan kan t.ex. finnas i en väska som polismannen bär med sig eller i polismannens rum eller bil.

Dold kroppsmikrofon används huvudsakligen av tre olika skäl (Rikspolisstyrelsens rapport *Teknikbundna spaningsmetoder*, 1996:4, s. 147). Metoden kan utgöra ett skydd för polismannen. Den kan också användas för att den som leder en viss spaningsoperation skall, av rättssäkerhetsskäl eller av polisoperativa skäl, ha möjlighet att följa händelseutvecklingen. Uppgifter som kommer fram vid användning av dold kroppsmikrofon kan vidare användas som underlag för spaning och som bevis inför domstol.

Polisen använder spaningsmetoden dold kroppsmikrofon relativt sällan. Den nödvändiga tekniska utrustningen finns endast på ett fåtal platser i landet. Beslut om att använda metoden fattas av den operative chefen och användningen av metoden dokumenteras inte särskilt.

Inspelning av telefonsamtal

En spaningsmetod som liknar användning av dold mikrofon är inspelning av telefonsamtal. Denna metod innebär att polisen spelar in telefonsamtal i vilka man själv deltar. Det kan också vara en

person som samarbetar med polisen som spelar in telefonsamtal i vilka han eller hon själv deltar.

Metoden används framför allt under medverkan av en målsägande och då alltid med dennes medgivande. Polisen tillhandahåller utrustning som möjliggör inspelning av samtal till och från målsägandens telefon, såväl telefoner kopplade till det fasta nätet som mobiltelefoner. Metoden används framför allt i samband med brotten utpressning och olaga hot. Den har tidigare använts i relativt liten utsträckning, men blir alltmer vanlig på grund av att de aktuella brottstyperna blir allt vanligare. Tekniken för denna spaningsmetod har förbättrats väsentligt. Metoden används framför allt på förundersökningsstadiet. Beslut om att använda metoden fattas då av förundersökningsledaren. Det dokumenteras att inspelningsutrustning har lånats ut till målsäganden.

Positionsbestämning (s.k. pejling)

Positionsbestämning (ofta benämnd pejling) är en metod som innebär att polisen spårar ett föremål genom att en elektronisk sändare fästs på föremålet. Sändaren kan fästas på t.ex. en bil. Det är också tekniskt möjligt att fästa sändaren på en väska eller kläder, varigenom en persons rörelser kan spåras. Signaler från sändaren tas emot av en mottagare och ger på så sätt information om var föremålet befinner sig och om det rör sig.

Polisen använder spaningsmetoden positionsbestämning i relativt stor utsträckning. Metoden används framför allt genom att sändare fästs på fordon och containrar. ”Pejling” av personer förekommer inte. Det är endast ett fåtal brottsbekämpande myndigheter som har tillgång till den tekniska utrustning som behövs, eftersom det krävs särskild kunskap för att använda utrustningen på rätt sätt och såväl utrustning som användningen av den behöver kvalitetssäkras. Beslut om att använda metoden fattas inom polisen av polischef eller av annan genom delegation av beslutanderätten. Att utrustning för positionsbestämning har monterats på aktuellt föremål dokumenteras regelmässigt.

10.4 Sammanfattning och bedömning

10.4.1 Inledning

Sedan en tid tillbaka pågår ett arbete med att förstärka och utveckla den brottsförebyggande delen av polisens brottsbekämpande verksamhet. För att kunna verka brottsförebyggande måste polisen inhämta och bearbeta information i större utsträckning än vad som sker vid det reaktiva arbetssätt som tidigare i större utsträckning präglade polisens arbete. Insamling och bearbetning av uppgifter måste också avse enskilda personer redan vid en låg grad av misstanke och omfatta även fall då misstankarna inte kunnat preciseras till att avse en viss specifik händelse eller gärning. Det ligger därför i sakens natur att en brottsförebyggande arbetsmetod innebär ett ökat intrång i den enskildes personliga integritet i förhållande till ett reaktivt arbetssätt.

Det finns inga allmänna bestämmelser som reglerar polisens rätt att inhämta information, vare sig i förhållande till andra myndigheter eller i andra sammanhang. Ett exempel på regler som uttryckligen ger polisen rätt att hämta in uppgifter är bestämmelserna om användning av straffprocessuella tvångsmedel i 27 och 28 kap. RB. Dessa bestämmelser är emellertid tillämpliga endast på förundersökningsstadiet. Under det spaningsskede som föregår en förundersökning är det således inte tillåtet att använda sig av t.ex. hemlig teleavlyssning.

För att fullgöra sin uppgift att förebygga brott samt att bedriva spaning och utredning av brott redan under ett inledande skede använder sig polisen av arbetsmetoder som förutsätter att tekniska hjälpmedel används och som i någon mån innebär att personer avlyssnas eller övervakas. Rätten att använda sådana metoder, som man tillsammans med manipulativa arbetsmetoder som provokation och infiltration har brukat inordna under den något diffusa benämningen *okonventionella spaningsmetoder*, är inte föremål för någon särskild reglering. Detsamma gäller andra former av spaningsmetoder som går ut på att övervaka personer. För denna typ av arbetsmetoder gäller dock, liksom för polisverksamheten i dess helhet, de allmänna principer som kommit till uttryck i 8 § polislagen. Där föreskrivs att en polisman som har att verkställa en tjänsteuppgift skall, under iakttagande av vad som föreskrivs i lag eller annan författning, ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter.

Avgörande för om en spaningsmetod skall anses tillåten är alltså i första hand att förfarandet inte omfattas av någon straffbestämmelse och inte heller av reglerna i rättegångsbalken om användning av tvångsmedel eller av andra föreskrifter som uttryckligen tar sikte på det aktuella förfarandet. De spaningsmetoder som polisen använder sig av, och som beskrivs i denna framställning, är inte föremål för någon sådan reglering och har därför ansetts i princip tillåtna. I det enskilda fallet har polis och åklagare att bedöma om spaningsåtgärden är förenlig med inte bara 8 § polislagen, utan också artikel 8 i Europakonventionen. Några författningsbestämmelser om vem som är behörig att fatta beslut beträffande denna typ av åtgärder och i vad mån en dokumentation skall ske finns inte.

Även spaningsmetoder som innebär att polisen använder sig av handmanövrerade kameror, dolda kroppsmikrofoner, inspelning av telefonsamtal och positionsbestämning har alltså ansetts i princip tillåtna. Som framgår av redovisningen ovan har rättsläget under senare år dock komplicerats av att vissa avgöranden av Europadomstolen har medfört att tveksamhet har uppstått i vad mån metoderna – i avsaknad av ett positivt lagstöd – är förenliga med artikel 8 i Europakonventionen.

JO är en av de instanser som uttalat tveksamhet huruvida de tekniska spaningsmetoderna är förenliga med artikel 8 i Europakonventionen, eftersom det i svensk rätt saknas regler som ger uttryckligt stöd för metodernas användning. I sitt remissyttrande över betänkandet *Ökad effektivitet och rättssäkerhet i brottsbekämpningen* (SOU 2003:74) framhåller JO att man i olika sammanhang har förordat en lagreglering såväl av s.k. pejling som användningen av handmanövrerade kameror och kroppsmikrofoner. Även Lagrådet anförde i sitt yttrande år 2000 över lagförslagen i remissen *Hemlig avlyssning m.m.* (prop. 2002/03:74 s. 99) att användningen av andra hemliga metoder för teknisk avlyssning och övervakning än de straffprocessuella tvångsmedlen, t.ex. kroppsmikrofoner och pejling, kunde komma i konflikt med artikel 8 om de inte var lagreglerade här.

Flera utredningar har under senare år förordat att en lagreglering införs för de tekniska spaningsmetoderna. Buggningsutredningen lade i sitt betänkande *Om buggning och andra hemliga tvångsmedel* (SOU 1998:46) fram förslag till lagreglering av polisens användning av dolda kroppsmikrofoner och inspelning av telefonsamtal. Utredningen förordade att också användningen av handmanövre-

rade kameror lagreglerades. Något lagstöd för användning av den pejling som förekom beträffande fordon och containrar behövdes enligt utredningen däremot inte.

Också 11-septemberutredningen förordade i betänkandet *Vår beredskap efter den 11 september* (SOU 2003:32) att lagregler infördes om användning av de nu aktuella spaningsmetoderna Därmed skulle enligt utredningen den rådande rättsosäkerheten undanröjas.

Beredningen för rättsväsendets utveckling har i betänkandet *Ökad effektivitet och rättssäkerhet i brottsbekämpningen* (SOU 2003:74) lagt fram förslag till en lagreglering som ger polisen rätt att vidta ”vilseledande eller dolda åtgärder” genom att använda handmanövrerad kamera, utrustning för avlyssning eller upptagning av samtal i vilket den som har utrustningen själv deltar, utrustning för positionsbestämning eller annat liknande tekniskt hjälpmedel. Flertalet remissinstanser tillstyrkte att en lagreglering sker.

10.4.2 Bör en reglering ske?

Spaningsmetoder som innebär att polisen genom användning av handmanövrerade kameror, dolda kroppsmikrofoner, inspelning av telefonsamtal, positionsbestämning och andra liknande metoder skaffar information om enskilda personer, är åtgärder som innebär någon form av avlyssning eller övervakning och som många gånger sker i hemlighet. Det står därför klart att sådana spaningsmetoder innefattar intrång i den enskildes integritet, dock naturligtvis i varierande grad beroende på hur den enskilda åtgärden genomförs.

Metoder av nämnt slag används redan av polisen och har ansetts i princip tillåtna, eftersom de inte omfattas av det straffbelagda området eller av annan lagstiftning som särskilt tar sikte på dessa förfaranden. Inte heller innefattar Europakonventionens bestämmelser om skydd för privat- och familjelivet, så som bestämmelserna hitintills har tolkats av Europadomstolen något generellt förbud för dessa metoder. Den relevanta frågan är därmed huruvida och i vad mån en författningsreglering av tekniska och andra integritetskänsliga metoder bör komma till stånd.

Oavsett hur Europakonventionen kan komma att tolkas, har det inte minst från polisen själv framställts önskemål om en reglering av de tekniska spaningsmetoderna. Gällande rättsläge innebär att det i det enskilda fallet är polis eller åklagare som skall avgöra om

en sådan åtgärd, eller någon annan integritetskänslig spaningsmetod, är förenlig med artikel 8 i Europakonventionen. Man har ansett att det inte är rimligt att det skall ankomma på en polismyndighet eller t.o.m. på den enskilde polismannen att göra sådana grannlaga överväganden som det här blir frågan om. Det uppstår då risk för att viktiga och värdefulla spaningsmetoder av försiktighetsskäl inte kommer till användning, vilket kan medföra negativa konsekvenser för polisens brottsförebyggande och brottsutredande arbete (se t.ex. Rikspolisstyrelsens remissvar över SOU 2003:74).

Även om man alltså från polisens sida anför framför allt effektivitetsskäl för en reglering, kan skäl för en reglering av tekniska och andra integritetskänsliga spaningsmetoder anföras också med hänsyn till behovet av att säkerställa skyddet för den enskildes integritet. Det kan inte anses tillfredsställande att det har uppstått en tveksamhet kring huruvida svensk rätt i detta avseende uppfyller kraven i artikel 8 i Europakonventionen. Beslut från JO och JK visar också att användandet av vissa spaningsmetoder kan innebära sådana intrång i den enskildes integritet att metoderna, när de används vid myndighetsutövning, bör ha stöd i lag. JO har i detta sammanhang framhållit att den omständigheten att svensk lag saknar regler om förfaranden av aktuellt slag inte kan innebära att det alltid är godtagbart att en befattningshavare vid en myndighet vidtar en sådan åtgärd. Som redovisats tillstyrker flertalet remissinstanser förslaget från Beredningen för rättsväsendets utveckling att en lagreglering införs. Många av dessa anför rättssäkerhets- och integritetsskyddshänsyn som skäl för en reglering.

Det bör också framhållas att den tekniska utvecklingen går mycket snabbt. De tekniska spaningsmetoderna blir därmed allt effektivare, vilket å andra sidan kan medföra att de blir mer känsliga från integritetsskyddssynpunkt. Som exempel kan nämnas att det i dag finns teknik för att ”pejla” mobiltelefoner i syfte att identifiera teleadresser. Metoden ger på ett relativt enkelt sätt uppgift om vilka tekniska hjälpmedel som finns inom ett begränsat geografiskt område och vilka telefonnummer, koder eller andra teleadresser som används. Beredningen för rättsväsendets utveckling har föreslagit att det straffprocessuella tvångsmedlet hemlig teleövervakning i 27 kap. 19 § RB skall omfatta även denna metod (SOU 2005:38, s. 208 f.).

Genom en reglering kan det klargöras vilka metoder, eller vilka komponenter i en metod, som är särskilt känsliga från integritetsskyddssynpunkt. Särskilda skyddsregler kan därmed uppställas för

sådana åtgärder och det kan avgöras huruvida en viss metod kan få användas också beträffande icke misstänkta personer. En uttrycklig reglering innebär också att det klargörs vem som är behörig att fatta beslut om åtgärden och i vilken utsträckning dokumentation skall ske. I detta sammanhang kan nämnas att det i förarbetena till polislagen (SOU 1982:63 s. 143) anfördes att spaningsmetoder av nu aktuellt slag alltid borde beslutas av åklagare eller polisman i chefsbefattning liksom att stränga krav på dokumentation måste upprätthållas. Av kartläggningen framgår att det varierar från metod till metod på vilken nivå beslut fattas och i vilken utsträckning dokumentation sker. En reglering innebär att en enhetlig ordning införs både för dessa och andra frågor som rör användningen av integritetskänsliga spaningsmetoder.

Sammanfattningsvis finns det utifrån ett hänsynstagande till skyddet för den enskildes personliga integritet starka skäl att förorda att integritetskänsliga spaningsmetoder blir föremål för en reglering.

10.4.3 Hur bör en reglering utformas?

En reglering av polisens spaningsmetoder väcker frågor inte bara från integritetsskyddssynpunkt. Också rättssäkerhetsaspekter måste beaktas. Därutöver måste självfallet hänsyn tas till att polisen skall kunna utföra sina uppgifter av brottsutredande och brottsförebyggande slag. I detta sammanhang kan frågor uppstå om hur olika delar av polisverksamheten skall avgränsas i förhållande till varandra. En reglering innebär också att gränsdragningsfrågor uppstår i förhållande till de straffprocessuella tvångsmedlen som regleras i 27 och 28 kap. rättegångsbalken. Ett exempel på detta är att de nu aktuella spaningsmetoderna inte används bara under det s.k. spaningsskedet, utan också under förundersökning. Till detta kommer att konvergensen på kommunikationsområdet, som innebär att olika kommunikationssätt genom datorer, fax, och telefoner hänger ihop med varandra via bl.a. radionät på marken, satelliter, koppartrådsnät och optiska fibernät, kan ge anledning att ifrågasätta om den åtskillnad är ändamålsenlig som i svensk rätt har gjorts mellan olika kommunikationssätt beträffande vad som kräver uttryckligt lagstöd och inte kräver detta.

Sammanfattningsvis kan sägas att en reglering av polisens spaningsmetoder väcker många andra frågor än integritetsskydds-

frågor och att dessa har sådana dimensioner att det inte kan anses ankomma på Integritetsskyddskommittén att på något mer preciserat sätt ta ställning till dem. Kommittén vill dock, för att något föra frågan framåt, peka på några aspekter från integritetsskyddssynpunkt som det är viktigt att beakta vid en översyn som tar sikte på att en reglering skall införas.

Vad som därvid i första hand kommer i blickpunkten är att en reglering inte kan syfta till att reglera *alla* spaningsmetoder som polisen använder sig av. En reglering bör syfta till att skilja ut de metoder som är särskilt känsliga från bl.a. integritetsskyddssynpunkt och där särskilt stränga krav bör gälla. I första hand bör en reglering ta sikte på de metoder som innebär att information hämtas in genom någon form av hemlig avlyssning eller övervakning. När det gäller övervakning är det emellertid inte givet att enbart åtgärder som utförs i hemlighet bör omfattas av en reglering. Även en ”öppen” övervakning som har ett inslag av tvång eller som bedrivs under lång tid kan vara särskilt integritetskänslig. En reglering bör vidare vara så teknikneutral som möjligt och undvika att söka uttömmande ange vilka metoder som avses.

Det kan finnas former av tekniska spaningsmetoder som från integritetsskyddssynpunkt är så ingripande att de endast bör vara tillåtna inom ramen för en förundersökning och därmed omfattas av bestämmelserna om tvångsmedel i rättegångsbalken. Genom en reglering kan det alltså klargöras att sådana spaningsåtgärder inte är tillåtna utanför en förundersökning. Ett exempel på en spaningsåtgärd som kan anses särskilt ingripande från integritetsskyddssynpunkt är positionsbestämning genom att sändare fästs på en person eller på ett föremål som en person bär med sig. Även positionsbestämning som förutsätter att ett intrång i egendom görs förefaller vara särskilt känslig från integritetsskyddssynpunkt. En sådan åtgärd torde i själva verket innebära att det straffbelagda området beträdes.

Om en reglering av polisens spaningsmetoder införs innebär det också att man i det sammanhanget kan ta ställning till vilka brottsbekämpande myndigheter som skall ha rätt att använda sig av metoderna.

Som framgått ovan innebär förslaget från Beredningen för rättsväsendets utveckling att en reglering av de tekniska spaningsmetoderna sker i form av lag. Kommittén anser sig för sin del inte behöva ta ställning till på vilken normnivå en reglering skall ske. Utgångspunkten för överväganden i denna fråga torde dock vara 8

kap. 3 § RF där det anges att föreskrifter om förhållandet mellan enskilda och det allmänna, som avser ingrepp i enskildas personliga eller ekonomiska förhållanden, meddelas genom lag.

10.4.4 Den allmänna frågan om polisens rätt till information

Polisrättsutredningen väckte i betänkandet *Tvångsmedel* (SOU 1995:47) frågan om allmänna regler för polisens rätt att inhämta information, t.ex. i förhållande till andra myndigheter (s. 177 f.). I lagrådsremissen *Hemlig avlyssning m.m.* avstod regeringen från att gå vidare med Buggningsutredningens förslag om en lagreglering av vissa tekniska spaningsmetoder eftersom man bl.a. ansåg att denna fråga hade samband med vad Polisrättsutredningen hade anfört.

Frånvaron av allmänna regler som ger polisen rätt att inhämta information innebär att polisen i första hand har möjlighet att skaffa information inom olika delar av samhället i samma utsträckning som gäller för envar. Samtidigt har polisen i dessa fall inte getts någon längre gående rätt att inhämta information än vad gemene man har, utan integritetshänsyn har ansetts ha samma tyngd i förhållande till polisen som till envar. Intresset av skydd för den enskildes integritet har emellertid i vissa särskilda fall fått stå tillbaka för polisens intresse att få information. Ett sådant exempel är polisens rätt enligt rättegångsbalken att efter domstolsbeslut få använda hemliga tvångsmedel. Sekretesslagens regler om att myndigheter under vissa omständigheter får lämna uppgifter till brottsutredande myndigheter utan hinder av sekretess är ett annat exempel.

En reglering som syftar till att polisen mer allmänt ges en bättre rätt än vad som gäller för envar att inhämta information, skulle innebära att polisens intresse av att skaffa information i större utsträckning ges företräde framför intresset att skydda den enskildes integritet. Resultatet skulle alltså kunna bli en generell försvagning av skyddet för den enskildes integritet när det gäller information som finns att hämta på olika samhällsområden. Från integritetsskyddssynpunkt kan en reglering av detta slag inte förordas.