Ett samlat ansvar för tillsyn över den personliga integriteten

Betänkande av
Utredningen om tillsynen över
den personliga integriteten

Stockholm 2016

STATENS OFFENTLIGA UTREDNINGAR

SOU 2016:65

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

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

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

ISBN 978-91-38-24503-3
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 22 december 2014 att tillkalla en särskild utredare med uppdrag att överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet (dir. 2014:164). Genom tilläggsdirektiv den 17 december 2015 beslutade regeringen om förlängd utredningstid (dir. 2015:139).

Som särskild utredare förordnades den 4 mars 2015 justitiekanslern Anna Skarhed.

Som experter att biträda utredningen förordnades den 18 mars 2015 advokaten Per Furberg, chefsjuristen vid Datainspektionen Hans-Olof Lindblom, juristen och ställföreträdande enhetschefen vid Post- och telestyrelsen Staffan Lindmark, professorn vid Stockholms universitet Cecilia Magnusson Sjöberg, kanslichefen vid Säkerhets- och integritetsskyddsnämnden Eva Melander Tell, rättssakkunniga vid Justitiedepartementet Linda Rantén, kammarrättsrådet vid Kammarrätten i Stockholm Elisabet Reimers samt ämnesrådet vid Justitiedepartementet David Törngren. Den 10 september 2015 entledigades David Törngren och förordnades som expert rättssakkunniga vid Justitiedepartementet Mattias Råbe.

Som sekreterare anställdes från och med den 20 april 2015 föredraganden i riksdagens konstitutionsutskott Jenny Jonasson.

Utredningen överlämnar härmed betänkandet *Ett samlat ansvar för tillsyn över den personliga integriteten* (SOU 2016:65). Experterna har ställt sig bakom utredningens överväganden och förslag. Betänkandet har därför formulerats i vi-form. Skilda uppfattningar i enskildheter och beträffande formuleringar kan dock ha före-

kommit utan att detta har gett anledning till något särskilt yttrande.

Uppdraget är härmed slutfört.

Stockholm i september 2016

Anna Skarhed

/Jenny Jonasson

Innehåll

Bilagor

Sammanfattning

Bakgrund

I vårt moderna och teknikutvecklade samhälle behandlas personuppgifter dagligen i en mycket stor omfattning, av både privatpersoner, företag och myndigheter. Överföringen av personuppgifter mellan aktörer i olika länder ökar också i omfattning. Samtidigt som sådan behandling ofta medför en positiv förenkling och effektivisering, och många gånger är nödvändig för att en verksamhet ska kunna bedrivas ändamålsenligt, medför all personuppgiftsbehandling risker för intrång i den enskildes personliga integritet. Uppgifter som av den enskilde kan uppfattas som känsliga och integritetskränkande kan t.ex. behandlas i olika slags register, uppkomma genom kameraövervakning eller publiceras i inlägg på internet. För att skydda enskildas integritet finns därför ett behov av bestämmelser som bland annat begränsar vilka personuppgifter som får behandlas och för vilka ändamål, och som föreskriver att en otillåten behandling ska rättas eller upphöra. Det är vidare viktigt att de personuppgiftsansvariga har tillräcklig kunskap om gällande bestämmelser kring personuppgiftsbehandling och att det finns en fungerande ordning som verkar för att bestämmelserna följs.

Dessa behov kan delvis tillgodoses genom en väl fungerande tillsyn, som därmed bidrar till att skyddet för den enskildes personliga integritet stärks. I de fall personuppgifter har behandlats på ett otillåtet sätt kan tillsynen också innebära t.ex. att den enskilde får felaktiga uppgifter rättade och tillerkänns kompensation i form av skadestånd, eller att den personuppgiftsansvarige föreläggs att upphöra med en felaktig behandling.

Den alltmer omfattande behandlingen av personuppgifter också på en internationell nivå har inte minst inom EU lett till ett ökat fokus på behovet av skydd för den enskildes personliga integritet. I

EU:s nyligen genomförda dataskyddsreform har frågor om tillsyn och tillsynsmyndigheternas befogenheter ett ökat fokus.

Vårt uppdrag

I vårt uppdrag har ingått att kartlägga den tillsyn över behandling av personuppgifter som i dag bedrivs av dels en central tillsynsmyndighet med ett övergripande tillsynsansvar, dels några andra myndigheter med ett tillsynsansvar inom avgränsade sakområden. Vi har dessutom haft i uppdrag att analysera för- och nackdelar med ett i högre grad samlat tillsynsansvar och att utreda hur skyddet för den enskildes personliga integritet kan förstärkas genom att tillsynen över behandling av personuppgifter i högre grad samlas hos en myndighet. Härutöver har vi haft att lämna förslag som innebär att Sverige lever upp till vissa av de krav som ställs på nationella tillsynsmyndigheter i den dataskyddsförordning och det nya dataskyddsdirektiv som har blivit resultatet av EU:s dataskyddsreform.

Den granskning av behandling av personuppgifter som bedrivs vid Statens inspektion för försvarsunderrättelseverksamheten (Siun) har inte omfattats av vårt uppdrag.

Uppdraget i sin helhet framgår av utredningens direktiv (bilaga 1 och 2).

I det följande redovisar vi en sammanfattning av våra överväganden och förslag. Vi kan dock redan nu konstatera att våra förslag har en stark koppling till frågor som regleras i de nyligen beslutade EU-rättsakterna på dataskyddsområdet. Detta innebär att de utredningar som har i uppdrag att föreslå vilka anpassningar som är nödvändiga med anledning av rättsakterna kan ha anledning att på nytt överväga de frågor som omfattas av vårt uppdrag.

Är det möjligt att samla all tillsyn hos en myndighet?

Vi har i enlighet med uppdraget genomfört en kartläggning av dagens tillsyn över behandling av personuppgifter. Kartläggningsarbetet redovisas i kapitel 6. Vi har valt att uppfatta uppdraget så att kartläggningsarbetet på ett så heltäckande sätt som möjligt ska redovisa alla de myndigheter som åtminstone teoretiskt kan sägas ha ett tillsynsuppdrag som omfattar behandlingen av personupp-

gifter i den granskade verksamheten. Det innebär att kartläggningen omfattar inte bara myndigheter som exempelvis Datainspektionen och Säkerhets- och integritetsskyddsnämnden (SIN), som helt eller till stor del ägnar sig åt tillsyn över personuppgiftsbehandling. Några av de myndigheter som ingår i redovisningen har ett huvudsakligt tillsynsuppdrag inom helt andra områden än dataskydd och skyddet för den personliga integriteten. Ytterligare några är inte huvudsakligen tillsynsmyndigheter utan har tilldelats ett visst tillsynsansvar utöver sina andra uppgifter.

I kapitel 8 redovisar vi våra iakttagelser med anledning av kartläggningen. Det gäller bland annat frågan om var det finns gränsdragningsproblem mellan olika myndigheters tillsynsuppdrag, och våra slutsatser när det gäller vilka för- och nackdelar det skulle innebära att samla all tillsyn över behandling av personuppgifter hos en myndighet.

Vår kartläggning visar att den centrala tillsynsmyndigheten Datainspektionen har ett mycket brett och omfattande tillsynsområde som innefattar personuppgiftsbehandling inom både privat och offentlig verksamhet. Datainspektionen har behörighet att utöva tillsyn över all behandling av personuppgifter. Utöver renodlad tillsynsverksamhet bedriver Datainspektionen ett förebyggande arbete som syftar till att öka kunskapen om de bestämmelser som ska skydda den enskildes personliga integritet vid behandling av personuppgifter. Om de personuppgiftsansvariga har god kännedom om vad som gäller vid personuppgiftsbehandlingen ökar förutsättningarna för ett gott integritetsskydd utan behov av ingripanden från en tillsynsmyndighet.

Vid sidan av Datainspektionens tillsyn utövar en handfull andra myndigheter tillsyn över sådan personuppgiftsbehandling som förekommer i vissa särskilda verksamheter. Tillsynen kompletterar eller ersätter här Datainspektionens tillsyn. Ett sådant tillsynsansvar har bland annat Post- och telestyrelsen (PTS), SIN, Konsumentverket, Centrala etikprövningsnämnden och länsstyrelserna.

Vi har kunnat konstatera vissa brister när det gäller fördelningen av tillsynsansvar mellan Datainspektionen å ena sidan och PTS, SIN, Centrala etikprövningsnämnden samt Inspektionen för vård och omsorg (IVO) å den andra. Lagstiftningen är vidare i några fall utformad på ett sådant sätt att några myndigheter kan sägas ha ett i vart fall teoretiskt tillsynsansvar även över behandling av person-

uppgifter, trots att tillsynen i dessa fall i realiteten uteslutande bedrivs av Datainspektionen och något annat inte torde ha varit avsikten.

Vi har övervägt om ett ännu mera samlat tillsynsansvar skulle kunna vara en fördel när det gäller effektivitet, resursutnyttjande och enhetlighet i tillsynsarbetet. Om det bara fanns en enda myndighet som hade ansvar för tillsynen av den personliga integriteten skulle det onekligen vara tydligt vilken myndighet som bär ansvaret. Det skulle också kunna ses som en fördel för tillsynsobjekten om en mera samlad tillsyn innebar att de skulle slippa bli föremål för tillsyn från olika håll.

Vår kartläggning visar emellertid att tillsynen redan i dag till stor del är samlad hos en myndighet, Datainspektionen, som också har ett övergripande ansvar när det gäller skyddet för den personliga integriteten. Att även ett antal andra myndigheter har ett till vissa områden avgränsat tillsynsansvar har ofta motiverats med att den personuppgiftsbehandling det då handlar om utgör en del av och har en naturlig och nära koppling till den verksamhet som i övrigt är föremål för myndighetens ansvarsområde och tillsyn. Detta gäller exempelvis för den tillsyn som utförs av PTS, Konsumentverket och Lotteriinspektionen. Den personuppgiftsbehandling som är föremål för särskild tillsyn, utöver eller vid sidan av den tillsyn som utförs av Datainspektionen, kan vidare avse en verksamhet där det har ansetts att det krävs speciell kunskap om och erfarenhet av den granskade verksamheten. Tillsynen är i dessa fall inriktad på områden som kan ge upphov till särskilda risker från integritetssynpunkt. Detta gäller den tillsyn som utförs av SIN. Det kan dessutom vara omöjligt att särskilja de åtgärder som innebär att en personuppgift har behandlats från andra åtgärder som också är föremål för en viss myndighets tillsyn. De behandlingsregler i lagen om elektronisk kommunikation (2003:389) som är föremål för tillsyn av PTS kan exempelvis, men behöver inte, innehålla personuppgifter som går att koppla till en fysisk person.

Sammanfattningsvis tydliggör kartläggningen att behandling av personuppgifter i dag förekommer inom alla delar av samhället, i en mycket stor omfattning och i mycket varierande typer av verksamheter. Det är när det gäller viss sådan verksamhet värdefullt och rent av nödvändigt att tillsynen bedrivs av en myndighet som har särskilda expertkunskaper på det område där behandlingen äger rum. Att uppdra åt en enda myndighet att utöva tillsyn över all per-

sonuppgiftsbehandling, oavsett i vilket sammanhang och i vilken verksamhet den förekommer, skulle enligt vår bedömning inte ge ett bättre skydd för enskildas personliga integritet. Man skulle i stället gå miste om fördelarna med att inom vissa för enskildas personliga integritet särskilt viktiga områden kunna utnyttja expertmyndigheternas kunskap om de granskade verksamheterna. Till detta kommer att det många gånger inte ens är möjligt att särskilja åtgärder som innebär att personuppgifter behandlas från andra åtgärder som också är föremål för tillsyn.

Vår slutsats är därför att det inte är möjligt eller ens lämpligt att samla all tillsyn över behandling av personuppgifter hos en enda myndighet. Datainspektionen bör även i fortsättningen vara den centrala myndigheten när det gäller personuppgiftsbehandling, men viss tillsyn härutöver även i fortsättningen utföras av andra myndigheter.

Även om vi alltså inte föreslår att all tillsyns ska utföras av en enda myndighet har vi övervägt frågan om det finns skäl att ge Datainspektionen ett nytt namn för att därigenom betona myndighetens roll som den centrala tillsynsmyndigheten när det gäller skyddet av den personliga integriteten. Vi har emellertid efter att ha vägt för- och nackdelarna med ett namnbyte stannat för att inte lägga fram ett sådant förslag.

Vissa anpassningar till EU:s dataskyddsreform

Den nya allmänna dataskyddsförordningen[1] och ett nytt direktiv om skydd för personuppgifter på det brottsbekämpande området[2] har antagits av Europaparlamentet och rådet. Förordningen ska börja tillämpas den 25 maj 2018 och direktivet ska vara implementerat senast den 6 maj 2018. Både förordningen och direktivet innehåller nya och utvidgade regleringar som gäller de nationella tillsynsmyndigheterna. Vi redovisar i kapitel 9 våra överväganden i

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (i detta betänkande kallat dataskyddsförordningen).
[2] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter (i detta betänkande kallat [det nya] dataskyddsdirektivet).

de delar av uppdraget som gäller vissa anpassningar efter förordningens och direktivets bestämmelser om tillsyn.

Svensk rätt uppfyller enligt vår bedömning dataskyddsförordningens och det nya dataskyddsdirektivets krav på att tillsynsmyndigheten ska vara fullständigt oberoende. Vi föreslår att Datainspektionen ska utses till svensk nationell tillsynsmyndighet enligt både förordningen och direktivet. Som sådan ska Datainspektionen delta i det arbete som kommer att bedrivas av den europeiska dataskyddsstyrelsen. Detta bör regleras i myndighetens instruktion.

Svensk rätt motsvarar dessutom i allt väsentligt enligt vår bedömning de krav som dataskyddsförordningen och det nya dataskyddsdirektivet uppställer om tillsynsmyndighetens organisation och utnämningen respektive avsättandet av tillsynsmyndighetens chef. Detta gäller bland annat kraven på ett öppet rekryteringsförfarande, skydd mot godtyckligt avskedande och förbud mot förtroendeskadliga bisysslor, där allmänna författningsregleringar redan finns. Vi föreslår härutöver att det införs en bestämmelse i myndighetens instruktion om att chefen för Datainspektionen anställs genom beslut av regeringen för en period om minst fyra år, med obegränsad möjlighet till förlängning.

Vi menar att det för närvarande saknas behov av att föreskriva att Datainspektionen ska ha ytterligare befogenheter utöver dem som följer av dataskyddsförordningen och att det inte finns något utrymme eller behov av en kompletterande reglering om myndighetens uppgifter i instruktionen. Vi föreslår, med hänvisning till EU-rättsakternas krav på tillsynsmyndighetens oberoende, att Datainspektionens instruktion inte längre ska ange att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud.

När det gäller Datainspektionens resursbehov med anledning av dataskyddsreformen konstaterar vi att det är för tidigt att mer exakt uppskatta storleken av resursbehovet. Det pågår ett arbete, både inom Datainspektionen och på annat håll, med att utreda och överväga vilka konsekvenser de nya rättsakterna får för hur tillsynen ska vara utformad i framtiden. Detta gäller inte minst de pågående utredningarna om anpassningar med anledning av dataskyddsförordningen och det nya dataskyddsdirektivet[3] som ska redo-

[3] Dir. 2016:15 och 2016:21.

visa sina överväganden nästa år. Mot bakgrund av de uppskattningar som i nuläget går att göra anser vi att Datainspektionens beräkningar bör ligga till grund för det fortsatta arbetet med att bedöma myndighetens resursbehov.

Förstärkning av skyddet för den enskildes personliga integritet genom vissa förändringar av tillsynsansvaret

Den omständigheten att vi inte ansett det vara till gagn för den personliga integriteten att samla all tillsyn hos en och samma myndighet hindrar inte att det inom den nuvarande myndighetsstrukturen kan finnas skäl att överväga en viss förändring av ansvarsfördelningen genom en överföring av tillsynsuppgifter mellan myndigheter. Våra överväganden i dessa dela redovisas i kapitel 10. Vi föreslår att tillsynsansvaret i några fall överförs från andra tillsynsmyndigheter till Datainspektionen. Genom att på detta sätt ytterligare samla tillsynsansvar hos Datainspektionen skapas enligt vår bedömning en mer ändamålsenlig tillsyn som ger ett starkare skydd för den enskildes personliga integritet. Problem med parallella tillsynsuppdrag kan härigenom undvikas och tillsynsuppgifter med ett naturligt samband kan samlas hos en och samma myndighet. Att tillsynen till viss del ytterligare samlas hos Datainspektionen stärker och tydliggör vidare myndighetens roll som central tillsynsmyndighet.

Vi föreslår mot denna bakgrund att tillsynen över bestämmelserna i lagen (2003:389) om elektronisk kommunikation om abonnentförteckningar och s.k. cookies ska utföras av Datainspektionen i stället för av PTS. Kopplingen till sektorn elektronisk kommunikation är här svagare och prövningen tar i stället sikte på mer allmänna dataskyddsrättsliga överväganden. Datainspektionen får härigenom ett mer samlat tillsynsansvar över behandling av personuppgifter. I tillsynsärenden som även i fortsättningen ska ligga kvar hos PTS kan enligt vår mening ett ökat samråd med Datainspektionen i frågor om innebörden av centrala dataskyddsrättsliga begrepp vara av värde. Det kan också bli aktuellt att hänskjuta frågor från PTS till Datainspektionen för avgörande. Möjligheterna till samråd och hänskjutande följer redan av lagstiftningen och kräver ingen ytterligare reglering. Även uppgifter som omfattas av sekretess torde enligt vår bedömning kunna lämnas över.

Vi föreslår vidare att tillsynen över den öppna polisens personuppgiftsbehandling i brottsbekämpande verksamhet inte längre ska ingå i SIN:s uppdrag utan i fortsättningen utföras endast av Datainspektionen. De praktiska problemen med parallella tillsynsuppdrag har när det gäller den öppna polisens personuppgiftsbehandling visat sig inte uppvägas av de fördelar för den personliga integriteten som man eftersträvade när SIN:s tillsynsuppdrag utvidgades till att även omfatta denna uppgift. Löpande kontakter och samordning i syfte att undvika kolliderande tillsynsinsatser tar i anspråk resurser hos båda myndigheterna som annars hade kunnat ägnas åt tillsyn. Det finns också en risk att de två myndigheterna kan komma till olika slutsatser i fråga om en viss typ av behandling eller, som en följd av beslutens olika karaktär, att Datainspektionens beslut efter överklagande ändras medan SIN:s i princip likalydande uttalande i samma fråga fortfarande gäller och inte kan överklagas. De båda myndigheterna har inte heller samma maktmedel till sitt förfogande när det gäller att säkerställa att tillsynen blir effektiv. Det är bara Datainspektionen som i dag har de befogenheter som såvitt vi nu kan bedöma krävs enligt det nya dataskyddsdirektivet.

Både Datainspektionen och SIN ska dock även i fortsättningen ha behörighet att utöva tillsyn över Säkerhetspolisens behandling av personuppgifter i brottsbekämpande verksamhet. Vi föreslår att SIN:s tillsyn därvid ska omfatta all personuppgiftsbehandling, inte bara sådan som följer av vissa lagar. Skyldigheten för SIN att i vissa fall göra en anmälan till Datainspektionen får anses gälla bara när det finns behov av ett rättsligt bindande och överklagbart beslut om exempelvis rättelse eller förbud mot fortsatt behandling. En sådan tolkning av omfattningen av SIN:s anmälningsskyldighet ryms enligt vår mening inom den nuvarande författningsregleringen.

Till skillnad från SIN har Datainspektionen i dag ingen skyldighet att på en enskilds begäran kontrollera lagenligheten av personuppgiftsbehandlingar. Det nya dataskyddsdirektivet kommer emellertid att medföra vissa sådana skyldigheter för den centrala tillsynsmyndigheten. Detta kommer att gälla även beträffande den personuppgiftsbehandling som sker hos andra myndigheter än Polismyndigheten. Vi anser att överväganden om den närmare utformningen av Datainspektionens skyldighet att på begäran av en enskild kontrollera om han eller hon har varit föremål för behandling av personuppgifter inom den öppna polisens brottsbekäm-

pande verksamhet bör göras av den utredning som har i uppdrag att genomföra direktivet i svensk rätt.

Våra förslag i denna del innebär att SIN:s verksamhet och uppdrag såvitt avser tillsyn över behandling av personuppgifter återgår till den ordning som gällde före 2012. Utöver tillsynen över Säkerhetspolisens personuppgiftsbehandling kommer SIN även i fortsättningen dessutom att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet, samt på begäran av en enskild kontrollera om han eller hon i strid med lag har utsatts för hemliga tvångsmedel eller varit föremål för Säkerhetspolisens personuppgiftsbehandling. SIN:s verksamhet består dessutom av de uppdrag som de två särskilda organen Registerkontrolldelegationen och Skyddsregistreringsdelegationen har.

Några ytterligare myndigheters tillsyn

Vi har kunnat konstatera att Datainspektionen och Centrala etikprövningsnämnden inte är helt överens om var gränsen går mellan de båda myndigheternas tillsynsansvar när det gäller forskning som innefattar behandling av personuppgifter. Vi har övervägt om oklarheterna bör åtgärdas genom en lagändring. Vi menar emellertid att ansvarsfördelningen framgår av den nuvarande lagstiftningen och dess förarbeten och att det därför saknas behov av någon ytterligare reglering. Datainspektionen ska utöva tillsyn över om den personuppgiftsbehandling som utförs inom ramen för viss forskning är förenlig med personuppgiftslagen, medan Centrala etikprövningsnämnden ska granska om forskning bedrivs i enlighet med etikprövningslagen. Det senare gäller även om forskningen innefattar behandling av personuppgifter.

Datainspektionen och IVO har ett delvis överlappande tillsynsansvar, men myndigheterna har i grunden helt olika uppdrag. För att tillgodose skyddet av den personliga integriteten vid behandling av personuppgifter i de verksamheter som omfattas av IVO:s tillsynsansvar är det viktigt att sådana frågor prövas av Datainspektionen. Det är därför angeläget att IVO samråder med Datainspektionen så snart det i IVO:s verksamhet uppkommer frågor om en viss personuppgiftsbehandlings lagenlighet. En sådan sam-

rådsskyldighet är redan författningsreglerad men vi konstaterar att det finns behov av att den upprätthålls och utvecklas.

Den rättsliga regleringen är som vi kunnat konstatera i vissa fall utformad så att den ger sken av att några ytterligare myndigheter ska utöva tillsyn även över behandling av personuppgifter trots att detta sannolikt inte medvetet varit avsikten. Myndigheterna ifråga utför inte heller i realiteten någon sådan tillsyn. Detta innebär emellertid inte att det uppkommer några brister i tillsynen över behandling av personuppgifter eller för skyddet av den personliga integriteten, eftersom tillsyn utförs av Datainspektionen även i dessa fall.

Slutligen konstaterar vi att det finns anledning att se över Datainspektionens tillsynsansvar enligt inkassolagen, i syfte att renodla och stärka Datainspektionens roll som central tillsynsmyndighet på området för integritetsskydd vid behandling av personuppgifter.

Frågan om ett integritetsskyddsråd

I vårt uppdrag har ingått att lämna förslag som innebär att den myndighet som ska ha det huvudsakliga ansvaret för tillsynen över behandling av personuppgifter är förberedd för att kunna fullgöra de uppgifter som Integritetskommittén (Ju 2014:09)kan komma att föreslå att ett integritetsskyddsråd ska ha.

Integritetskommittén redovisade i ett delbetänkande i juni 2016 (SOU 2016:41) sina överväganden bland annat i frågan om ett integritetsskyddsråd (bet s. 646 f.). Kommittén anser att det inte bör inrättas något integritetsskyddsråd med huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen. Kommittén konstaterar att Datainspektionen redan i dag har ett övergripande ansvar för skyddet av personuppgifter, vilket bland annat innebär att myndigheten regelmässigt är remissinstans (både när det gäller formella remisser och delningar från departementen) och ofta finns representerad i utredningar som gäller sådana frågor. Det finns enligt kommittén dessutom ett flertal andra myndigheter och organisationer, såsom Justitiekanslern, Riksdagens ombudsmän, Myndigheten för samhällsskydd och beredskap, PTS, SIN samt Advokatsamfundet, som också granskar förslag till ny lagstiftning ur ett integritetsskyddsperspektiv. Detta bidrar enligt

kommittén till att integritetsskyddsperspektivet lyfts fram i lagstiftningsarbetet och att bristfälliga avvägningar uppmärksammas.

Integritetskommittén föreslår emellertid att Datainspektionen ska få i uppdrag att årligen lämna en rapport till regeringen som sammanställer och analyserar den mest aktuella och betydelsefulla utvecklingen som påverkar den personliga integriteten. Regeringen ska därefter i sin tur överlämna rapporten till riksdagen i form av en skrivelse som också innehåller regeringens kommentarer till rapporten.

Vi har med anledning av Integritetskommitténs ställningstagande i denna del ansett att det inte finns skäl för oss att lämna förslag som gäller ett integritetsskyddsråds uppgifter.

Konsekvenser av våra förslag

Ett omfattande arbete pågår, både inom Regeringskansliet och i ett stort antal utredningar, som på olika sätt berör den personliga integriteten och tillsyn över behandling av personuppgifter. Detta arbete avser till stora delar anpassningar till EU:s nyligen beslutade dataskyddsreform. Resultatet kan komma att få betydelse för Datainspektionens och andra myndigheters arbete och organisation. Den nya dataskyddsförordningen och det nya dataskyddsdirektivet innehåller omfattande bestämmelser om de nationella tillsynsmyndigheternas uppgifter, befogenheter och inbördes samverkan, som såvitt vi kan bedöma kommer att innebära utökade uppgifter för främst Datainspektionen.

Det är mot denna bakgrund svårt att i nuläget göra annat än preliminära uppskattningar av de ekonomiska konsekvenserna av våra förslag. Genomförandet av våra förslag och de förslag som kan bli resultatet av övriga utredningar måste rimligen ske samordnat.

Det pågående arbetet med att även i andra utredningar analysera vilka anpassningar och författningsregleringar som är nödvändiga med anledning av EU:s dataskyddsreform, och nödvändigheten av att göra samlade överväganden om behovet och utformningen av författningsregleringar, innebär att vi nu inte lämnar något annat förslag om när våra föreslagna författningsförändringar bör träda i kraft än att senast maj 2018 framstår som en rimlig utgångspunkt.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs i fråga om lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.	
Nämnden ska även utöva tillsyn över den behandling av personuppgifter *enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten. När det gäller Säkerhetspolisen ska tillsynen även avse sådan behandling enligt polisdatalagen (1998:622).* Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § polisdatalagen (2010:361) *och 5 § polisdatalagen*	Nämnden ska även utöva tillsyn över *behandlingen* av personuppgifter *i Säkerhetspolisens brottsbekämpande verksamhet.* Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § polisdatalagen (2010:361).

(1998:622) samt 12 § lagen om polisens allmänna spaningsregister.

Denna lag träder i kraft den xxx.

1.2 Förslag till förordning om ändring av förordningen (2003:396) om elektronisk kommunikation

Härigenom föreskrivs i fråga om förordningen (2003:396) om elektronisk kommunikation att 2 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 §
Post- och telestyrelsen är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation.	Post- och telestyrelsen är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation. *Datainspektionen är dock tillsynsmyndighet såvitt avser 6 kap. 15, 16 och 18 §§ i den lagen.*

Post- och telestyrelsen ska för Sveriges del fullgöra de uppgifter som den nationella tillsynmyndigheten har enligt

1. Europaparlamentets och rådets förordning (EU) nr 531/2012 av den 13 juni 2012 om roaming i allmänna mobilnät i unionen, och

2. Europaparlamentets och rådets förordning (EU) nr 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster och förordning (EU) nr 531/2012 om roaming i allmänna mobilnät i unionen.

Denna förordning träder i kraft den xxx.

1.3 Förslag till förordning om ändring i förordning (2007:975) med instruktion för Datainspektionen

Härigenom föreskrivs i fråga om förordningen (2007:975) med instruktion för Datainspektionen att 1, 2 a, 4 och 5 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet.	
Myndigheten ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen (1998:204).	
Myndigheten ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.	
2 a §	
Myndigheten är tillstånds- och tillsynsmyndighet enligt kreditupplysningslagen (1973:1173) och inkassolagen (1974:182).	
Myndigheten är tillsynsmyndighet enligt *artikel 28 i 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, ändrat genom Europaparlamentets och rådets förordning (EG) nr 1882/2003.*	Myndigheten är tillsynsmyndighet enligt *– artikel 51.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), och*

	– artikel 41.1 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
	Myndigheten ska delta i den europeiska dataskyddsstyrelsens arbete.
	Myndigheten är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation såvitt avser 6 kap. 15, 16 och 18 §§ i den lagen.
	4 §
Myndigheten är nationell tillsynsmyndighet enligt	Myndigheten är nationell tillsynsmyndighet enligt
– artikel 114 i konventionen om tillämpning av Schengenavtalet av den 14 juni 1985 (Schengenkonventionen),	– artikel 114 i konventionen om tillämpning av Schengenavtalet av den 14 juni 1985 (Schengenkonventionen),
– artikel 24 i rådets beslut 2009/917/RIF av den 30 november 2009 om användning av informationsteknik för tulländamål (TIS-rådsbeslutet),	– artikel 24 i rådets beslut 2009/917/RIF av den 30 november 2009 om användning av informationsteknik för tulländamål (TIS-rådsbeslutet),
– artikel 33 i rådets beslut av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol),	– artikel 33 i rådets beslut av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol),
– artikel 30.5 i rådets beslut 2008/615/RIF av den 23 juni	– artikel 30.5 i rådets beslut 2008/615/RIF av den 23 juni

2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet),

– artikel 41 i Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen),

– artikel 7.1 och 7.2 i Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott (CBE-direktivet), i den ursprungliga lydelsen,

– artikel 8.5 i rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (VIS-rådsbeslutet), *och*

– artikel 25.1 i rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet).

2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet),

– artikel 41 i Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen),

– artikel 7.1 och 7.2 i Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott (CBE-direktivet), i den ursprungliga lydelsen, *och*

– artikel 8.5 i rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (VIS-rådsbeslutet).

	5 §
Myndigheten leds av en myndighetschef.	Myndigheten leds av en myndighetschef, *som anställs genom beslut av regeringen för en period om minst fyra år. Anställningen får förlängas.*

Denna förordning träder i kraft den xxx.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Av våra direktiv[1] framgår att det övergripande målet för vårt uppdrag har varit att stärka skyddet för den enskildes personliga integritet. Direktiven konstaterar att ansvaret för tillsyn på integritetsområdet i dag ligger på flera myndigheter. I syfte att stärka skyddet för den personliga integriteten har vi haft i uppdrag att överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet. I detta uppdrag har ingått att kartlägga den tillsyn som i dag bedrivs av flera myndigheter och att analysera fördelar och nackdelar med att samla detta tillsynsansvar i en myndighet. Härutöver har vi haft i uppdrag att lämna förslag som innebär att en tillsynsmyndighet är förberedd för att kunna fullgöra de uppgifter som Integritetskommittén (Ju 2014:09) kan komma att föreslå att ett integritetsskyddsråd ska ha. Våra förslag ska så långt som möjligt vara anpassade efter resultatet av EU:s pågående reform på dataskyddsområdet. Denna senare del av uppdraget har under arbetets gång preciserats och utvidgats genom att det i direktiven till två andra utredningar[2] har angetts vilka frågor om anpassningar till de nya rättsakternas bestämmelser om de nationella tillsynsmyndigheterna som ska anses falla inom vårt uppdrag.

[1] Direktiven (dir. 2014:164) beslutades den 22 december 2014. I tilläggsdirektiv (dir. 2015:139) beslutade regeringen den 17 december 2015 om förlängd utredningstid. De båda direktiven bifogas i bilaga 1 och 2.
[2] Dir. 2016:15 med direktiv till Dataskyddsutredningen och dir. 2016:21 med direktiv till Utredningen om 2016 års dataskyddsdirektiv.

2.2 Utredningens arbete

Utredningen har haft åtta sammanträden med experterna, varav ett internatsammanträde. Dessutom har vi haft många underhandskontakter. Vi har haft kontakt och samråd med andra kommittéer och utredningar, främst Integritetskommittén (Ju 2014:09), Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten (Ju 2014:10), Dataskyddsutredningen (Ju 2016:04), Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) samt Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14). Vi har också varit i kontakt med många av de svenska myndigheter som har sådana tillsynsuppgifter som omfattas av vårt uppdrag, liksom med dataskyddsmyndigheterna i Norge, Danmark och Finland.

Organisationen Dataskydd.net har skrivit till utredningen.

3 Behandling av personuppgifter och skyddet av den personliga integriteten

3.1 Inledning

I vårt moderna och teknikutvecklade samhälle behandlas personuppgifter dagligen i en mycket stor omfattning, av både privatpersoner, företag och myndigheter. Sådan behandling utförs ofta som ett led i en verksamhet som ses som någonting positivt och är många gånger nödvändig för att verksamheter ska fungera ändamålsenligt och effektivt. All personuppgiftsbehandling medför dock samtidigt risker för intrång i den enskildes personliga integritet. Uppgifter som av den enskilde kan uppfattas som känsliga och integritetskränkande kan t.ex. behandlas i olika former av register, uppkomma genom kameraövervakning eller publiceras i inlägg på internet. För att skydda enskildas integritet finns därför ett behov av bestämmelser som bland annat begränsar vilka personuppgifter som får behandlas och för vilka ändamål och som föreskriver att en otillåten behandling ska rättas eller upphöra.

I det följande beskrivs vad som menas med personlig integritet och behandling av personuppgifter, samt de bestämmelser i svensk och internationell rätt som syftar till att skydda den enskildes personliga integritet.

3.2 Skyddet av den personliga integriteten

3.2.1 Integritetsbegreppet

Den omfattande behandling av personuppgifter som dagligen försiggår omkring oss innebär risker för intrång i vad den enskilde kan uppfatta som privat och känsligt. Man brukar här tala om ett behov av skydd av den personliga integriteten. Ett sådant behov finns naturligtvis även när det inte är fråga om personuppgiftsbehandling utan om annan verksamhet som på något sätt kan upplevas som känslig för den enskilde.

Det finns inte i vare sig svensk eller internationell rätt någon enhetlig definition av begreppet personlig integritet. I flera sammanhang har försök att formulera en sådan definition övergetts med motiveringen att det inte låter sig göras, bland annat eftersom begreppets innebörd uppfattas så olika av olika personer och dessutom kan förändras med tiden, både som en följd av förändrade förutsättningar och förändrade attityder.[1] Dagens snabba teknikutveckling, med exempelvis s.k. smarta biljetter och övervakningskameror, torde dessutom kunna både öka den enskildes önskan och behov av att freda sig från intrång och, å andra sidan, göra att fler företeelser, som förr skulle ha uppfattats som oacceptabla intrång i den personliga integriteten, nu upplevs som normala och kanske till och med önskvärda. Ett exempel på detta är olika former av kameraövervakning, som i vissa situationer alltmer har kommit att uppfattas snarare som en trygghetsskapande säkerhetsåtgärd än som en integritetskränkning.

Det har emellertid inte ansetts nödvändigt att formulera en allmängiltig definition av begreppet personlig integritet för att kunna bedöma vilka intressen som har ett sådant skyddsvärde att de bör omfattas av ett särskilt skydd mot omotiverade ingrepp (prop. 2009/10:80 s. 175). Den svenska lagstiftningen tar i stället i hög grad sikte på att identifiera vilka gärningar eller företeelser som, efter att i en intresseavvägning ha ställts mot andra intressen, ska förbjudas eller begränsas eftersom de bedöms innebära en alltför stor kränkning av den personliga integriteten. Härutöver

[1] Se exempelvis Integritetsutredningen i SOU 2002:18 s. 52 f., Stig Strömholm i Svensk Juristtidning 1971 s. 675 och Integritetsskyddskommittén i SOU 2007:22 s. 53 f.

finns bestämmelser om vilka åtgärder som ska vidtas för att minimera risken för sådana kränkningar.

Det finns emellertid vissa beskrivningar av begreppet personlig integritet som de flesta kan enas om. Man talar således om en personlig sfär som den enskilde har rätt till och där ett ingrepp bör kunna avvisas.[2] Det talas också i olika sammanhang om ”privatlivets fred”,[3] och om rätten till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens (Europakonventionen). I EU:s stadga om de grundläggande rättigheterna föreskrivs bland annat en rätt till skydd för fysisk och mental integritet för sitt privatliv och familjeliv, sin bostad, sina kommunikationer och för sina personuppgifter, och i Finlands grundlag talas om rätten till skydd för privatliv, heder och hemfrid. Internationella juristkommissionen anordnade 1967 en nordisk konferens om privatlivets rättsskydd, som i en resolution slog fast att rätten till privatliv i allmänhet innebär en rätt för individen att leva sitt eget liv med ett minimum av inblandning från myndigheter, allmänhet och andra individer.

Den personliga sfär som avses när man pratar om personlig integritet kan vara fysisk och rumslig och då ge dels en rätt till skydd mot kränkningar av exempelvis den egna kroppen och bostaden, dels en rätt till rörelsefrihet. Den kan också avse materiell integritet i form av egendomsskydd. Härutöver kan man tala om personlig integritet i en mera ideell mening. Bestämmelser som ger ett skydd mot exempelvis insamling och registrering av uppgifter om en persons privata förhållanden, såsom politiska åsikter, ekonomi och var han eller hon har befunnit sig, tar sikte på den aspekten av den personliga integriteten. I linje med denna distinktion har också talats om fysisk respektive psykisk eller mental integritet.[4]

När det särskilt gäller personlig integritet vid automatiserad behandling av personuppgifter kan begreppet sägas ha fått en vidare innebörd i och med att också datakvalitets- eller datasäkerhetskrav bör tillgodoses. De uppgifter som behandlas ska med andra ord

[2] Se t.ex. Integritetsutredningen i betänkandet Personlig integritet i arbetslivet (SOU 2002:18 s. 52 f.), Integritetsskyddskommittén i delbetänkandet Skyddet för den personliga integriteten – kartläggning och analys (SOU 2007:22 s. 65) och prop. 2009/10:80 s. 175.
[3] Se exempelvis 1966 års Integritetsskyddskommittés betänkande Skydd mot avlyssning, (SOU 1970:47).
[4] Kommittén om genetisk integritet i betänkandet Genetik, integritet och etik (SOU 2004:20).

vara korrekta, och de får bara behandlas i rätt sammanhang och för berättigade ändamål.[5] Också hur personuppgifter t.ex. sparas och sprids kan ha, eller upplevas ha, negativa konsekvenser för den enskilde. En allmänt tillgänglig och sökbar samling med i och för sig relativt harmlösa personuppgifter kan upplevas som känslig av den enskilde, exempelvis för att den kan ge en bild av hur den enskilde lever sitt liv eller vad han eller hon har för intressen.

3.2.2 Behovet av skydd för den personliga integriteten vid behandling av personuppgifter

I dagens samhälle är det nödvändigt att personuppgifter får behandlas. Uppgifter om adresser, personnummer, beställda varor, begångna brott och mottagen socialhjälp är exempel på information som myndigheter och företag kan behöva behandla för att kunna fullgöra sina uppgifter och driva sin verksamhet. Tekniska hjälpmedel som t.ex. olika former av datoriserade register kan ge ökad effektivitet och säkrare beslutsunderlag.

För den enskilde kan det emellertid kännas både oroligt och olustigt att uppgifter om personliga förhållanden finns sparade och ibland kan vara tillgängliga för många. Och i fel händer kan känsliga personuppgifter användas på ett sätt som orsakar allvarlig skada. Det finns därför ett behov av bestämmelser som skyddar den personliga integriteten vid behandling av personuppgifter. Ett sådant skydd kan exempelvis innebära begränsningar i vilka uppgifter som får behandlas och för vilka ändamål, vem som ska ha rätt att ta del av uppgifterna – både genom begränsningar i behörigheten inom exempelvis en myndighet att behandla uppgifterna, och genom bestämmelser om sekretess eller informations-säkerhet – samt hur länge uppgifterna ska få sparas och hur överträdelser av reglerna ska sanktioneras. Det är en grundläggande dataskyddsrättslig regel att bara den som behöver en uppgift för att utföra en arbetsuppgift – den läkare som ska bedöma lämplig vård för en patient eller den tjänsteman vid Försäkringskassan som ska fatta beslut i ett ärende om en förmån – har behörighet att behandla de personuppgifter som är relevanta i det enskilda fallet. Andra läkare

[5] Personuppgiftslagsutredningen i betänkandet Översyn av personuppgiftslagen (SOU 2004:6 s. 30 f.).

eller tjänstemän på samma arbetsplats kan därmed sakna rätten att behandla personuppgifterna trots att de rent faktiskt har tillgång till dem, om de inte behöver dem för att utföra en arbetsuppgift. Dessutom finns krav på att de personuppgifter som behandlas ska skyddas genom lämpliga tekniska och organisatoriska säkerhetsåtgärder.

Behovet av skydd för den personliga integriteten måste å andra sidan vägas mot andra intressen i samhället. Av särskild betydelse är integritetsskyddets förhållande till värdet av tryck- och yttrandefrihet, särskilt när det gäller uppgifter som inhämtas för att spridas i grundlagsskyddade medier. Möjligheterna för det allmänna att ingripa på grund av innehållet i sådana medier är mycket begränsade och förutsätter att framställningen innebär ett missbruk av tryck- eller yttrandefriheten. När det gäller skyddet för den personliga integriteten utgör förtal, förolämpning och vissa hatbrott tryckfrihets- och yttrandefrihetsbrott. Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten har i februari 2016 föreslagit justeringar när det gäller vissa av dessa brott för att bättre anpassa dem till de nya typer av hot som har kommit att följa på den tekniska utvecklingen och framväxten av bland annat sociala medier (SOU 2016:7 s. 473 f.).

I detta sammanhang kan också nämnas de frivilliga pressetiska regler som antagits av ett stort antal svenska medier och som bland annat uppmanar till respekt för privatlivets helgd och försiktighet när det exempelvis gäller publicering av namn och bild.

I de följande avsnitten redovisas bestämmelser som avser att skydda den enskildes personliga integritet i svensk lagstiftning och i några internationella överenskommelser.

3.2.3 Svensk lagstiftning till skydd för den personliga integriteten

Den personliga integriteten skyddas i svensk rätt både i grundlag och i vanlig lag.

Regeringsformen

Det allmänna ska enligt 1 kap. 2 § fjärde stycket regeringsformen bland annat verka för att demokratins idéer blir vägledande inom samhällets alla områden och värna den enskildes privatliv och familjeliv. Bestämmelsen är en del av regeringsformens s.k. program- eller målsättningsstadganden. Placeringen i regeringsformens första kapitel, bland andra bestämmelser som gäller grunderna för det svenska statsskicket, markerar den vikt lagstiftaren har velat lägga vid dem. De utgör emellertid inte rättsligt bindande föreskrifter som kan grunda några krav eller anspråk på det allmänna. De anger i stället mål för den samhälleliga verksamheten och anses bekräfta inställningen att lagstiftaren och myndigheterna så långt som möjligt bör beakta den enskildes intresse av integritet.[6] Som målsättningsstadganden kan de få politisk betydelse och frågan om deras effekt kan bli föremål för politisk kontroll.[7]

Den enskildes integritet i vid mening skyddas i regeringsformens andra kapitel genom förbudet mot dödsstraff samt mot kroppsstraff, tortyr och medicinsk påverkan i syfte att framtvinga eller hindra yttranden (2 kap. 4 och 5 §§). Var och en är också i övrigt skyddad mot påtvingat kroppslig ingrepp, liksom mot kroppsvisitation, husrannsakan, brevkontroll och hemlig avlyssning samt åsiktsregistrering (2 kap. 3 § och 6 § första stycket). De senare bestämmelsernas skydd har emellertid inte primärt motiverats av hänsyn till den enskildes integritet utan främst av att skydda den fria åsiktsbildningen.[8] Av 2 kap. 15 § regeringsformen följer vidare ett egendomsskydd genom ett skydd mot tvångsexpropriation. Om egendom trots allt exproprieras, vilket ska vara

[6] Holmberg m.fl., Grundlagarna (3 uppl. 2012), s. 61.
[7] Prop. 1973:90 s. 194 f., prop. 1975/76:209 s. 128 och SOU 1975:75 s. 184.
[8] SOU 1975:75 s. 134 f.

möjligt för att tillgodose angelägna allmänna intressen, ska den enskilde som huvudregel få full ersättning för sin förlust.

Tidigare föreskrevs det i 2 kap. 3 § andra stycket regeringsformen att varje medborgare, i den utsträckning som närmare angavs i lag, skulle skyddas mot att hans eller hennes personliga integritet kränktes genom att uppgifter om honom eller henne registreras med hjälp av automatisk databehandling. Den 1 januari 2011 ersattes denna bestämmelse av 2 kap. 6 § andra stycket regeringsformen, enligt vilken var och en är skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Bestämmelsen infördes sedan Integritetsskyddskommittén i sitt slutbetänkande Skyddet för den personliga integriteten – Bedömningar och förslag (SOU 2008:3) anfört att det var en brist att det på grundlagsnivå saknades bestämmelser om skydd för den personliga integriteten som på ett mer påtagligt sätt balanserade de övriga grundlagsreglerade fri- och rättigheterna. En svag förankring av skyddet för den personliga integriteten i grundlagen kunde enligt kommittén innebära att integritetsskyddsaspekterna inte gavs tillräcklig vikt när ny lagstiftning arbetades fram. Ett utvidgat materiellt grundlagsskydd för den personliga integriteten borde enligt kommittén ta sikte på från integritetssynpunkt särskilt skyddsvärda områden, dvs. områden där det är särskilt motiverat att begränsa lagstiftarens handlingsfrihet när det gäller i vilken utsträckning och i vilken form intrång kan tillåtas (bet. s. 255 f.).

Grundlagsutredningen, som redovisade sitt uppdrag ett knappt år efter Integritetsskyddskommittén, ansåg att det var angeläget att grundlagsskyddet för den personliga integriteten stärktes och föreslog att en bestämmelse i linje med Integritetsskyddskommitténs förslag infördes i regeringsformen (SOU 2008:125 s. 473 f.). Regeringen anförde i propositionen att respekten för individens självbestämmande är grundläggande i en demokrati. Genom att på grundlagsnivå stärka skyddet för den personliga integriteten, utan att detta skyddsintresse i första hand värderas utifrån intresset av att skydda den fria åsiktsbildningen, kommer vikten av respekt för individens rätt att själv förfoga över och ta ställning till det all-

männas tillgång till sådan information som rör hans eller hennes privata förhållanden att betonas på ett tydligare sätt.[9]

Uttrycket personliga förhållanden i den nya bestämmelsen ska anses ha samma innebörd som i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400), förkortad OSL.[10] Det innebär att regleringen omfattar information av vitt skilda slag, såsom uppgifter om namn och andra personliga identifikationsuppgifter, adress, familjeförhållanden, hälsa och vandel. Även fotografiska bilder och uppgifter som inte är direkt knutna till den enskildes privata sfär, t.ex. uppgifter om en anställning, omfattas av uttrycket, liksom uppgifter om den enskildes ekonomi.

Den nu arbetande Integritetskommittén (Ju 2014:09) har bland annat i uppdrag att genomföra en uppföljning av hur denna reform av grundlagsskyddet har fallit ut. Uppföljningen bör enligt kommitténs direktiv innefatta en kartläggning och analys av de integritetsaspekter som har aktualiserats i lagstiftningsarbetet sedan den nya grundlagsbestämmelsen trädde i kraft. Kommittén, vars uppdrag behandlas ytterligare i kapitel 5, lämnade ett delbetänkande i juni 2016[11] och ska slutredovisa sitt uppdrag senast den 1 juni 2017 (dir. 2014:65 och 2016:12).

Skyddet mot döds- och kroppsstraff, tortyr och medicinsk påverkan i syfte att framtvinga eller hindra yttranden är absolut, dvs. dessa rättigheter får inte begränsas på annat sätt än genom en grundlagsändring. Skyddet mot de övriga begränsningarna av den personliga sfären, såsom kroppsvisitation, husrannsakan och intrång i övrigt som innebär övervakning och kartläggning av den enskildes personliga förhållanden, får begränsas genom lag. Sådana begränsningar får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett dem och heller inte sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen. Begränsningar får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 20 och 21 §§ regeringsformen).

[9] Prop. 2009/10:80 s. 176.
[10] A. prop. s. 177.
[11] Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén (SOU 2016:41).

Det relativt nya skyddet mot övervakning och kartläggning i 2 kap. 6 § andra stycket regeringsformen, och det faktum att begränsningar i skyddet endast får göras i lag, har bland annat inneburit att viss personuppgiftsbehandling som tidigare har reglerats i förordning numera regleras i lag.[12]

Personuppgiftslagen

Personuppgiftslagens (1998:204) syfte är att skydda enskilda mot kränkning av den personliga integriteten vid behandling av personuppgifter. Lagen innehåller bestämmelser som anger under vilka förutsättningar personuppgifter får behandlas. Överträdelser av bestämmelserna kan leda till skadeståndsansvar och i vissa fall också straff i form av böter eller fängelse. Lagen gäller all helt eller delvis automatiserad behandling av personuppgifter, oavsett om det är det allmänna eller en privat aktör som utför behandlingen. Rent privat behandling av personuppgifter, som exempelvis en privatpersons adressregister eller elektroniska dagbok, undantas dock. Även manuellt förda register eller liknande omfattas i vissa fall.

Med personuppgifter avses enligt personuppgiftslagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Uppgiften behöver inte avse sådant som kan betecknas som privat eller känsligt utan kan vara helt neutral, så länge den går att hänföra till en viss individ. Begreppet personuppgifter omfattar heller inte bara uppgifter i vanlig text. Även bilder och ljudupptagningar kan vara personuppgifter, liksom krypterade uppgifter eller olika slags elektroniska identiteter, såsom IP-adresser. En förutsättning är dock alltid att uppgifterna kan kopplas till en fysisk person som är i livet.

Med behandling av personuppgifter menas varje åtgärd eller serie av åtgärder som vidtas med dessa personuppgifter. Som exempel på sådana åtgärder nämns i personuppgiftslagen bland annat insamling, registrering, lagring, användning, utlämnande genom översändande och spridning eller annat tillhandahållande av uppgifter. I stort sett all hantering av personuppgifter, även att bara

[12] Som exempel kan nämnas domstolsdatalagen (2015:728) och utlänningsdatalagen (2016:27).

lämna ut eller ta del av en uppgift, omfattas därmed av begreppet behandling. Det krävs heller inte att uppgifterna sparas; även uppgifter som bara tillfälligt förekommer i digital form, t.ex. bildupptagningar i en webbkamera som visas på internet men som inte sparas, har ansetts utgöra behandling av personuppgifter.[13]

Personuppgiftslagen innehåller grundläggande krav på behandlingen av personuppgifter. Personuppgifter får exempelvis behandlas bara när det är lagligt och på ett korrekt sätt. Uppgifterna får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål, och de får inte sedan behandlas för något annat, oförenligt ändamål. Den som är ansvarig för behandlingen måste vidta alla rimliga åtgärder för att rätta eller ta bort felaktiga eller ofullständiga personuppgifter, liksom sådana uppgifter som inte längre behövs. Den enskilde måste som huvudregel samtycka till behandlingen av personuppgifter, om den inte är nödvändig för att exempelvis vissa lagstadgade skyldigheter ska kunna fullgöras eller vissa intressen ska kunna skyddas. Personuppgifter får också behandlas om den personuppgiftsansvariges berättigade intresse av en behandling vid en intresseavvägning väger tyngre än den registrerades intresse av integritetsskydd. De registrerades inställning till behandlingen ska beaktas vid intresseavvägningen. Om den registrerade motsätter sig en behandling av uppgifter om honom eller henne och invändningen anses vara sakligt motiverad bör den personuppgiftsansvariges intresse av att behandla uppgifterna enligt Datainspektionens praxis endast i undantagsfall anses väga över.[14]

Känsliga personuppgifter, dvs. uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening eller som rör hälsa eller sexualliv får som huvudregel enligt personuppgiftslagen inte behandlas. Behandling kan dock vara tillåten med den registrerades uttryckliga samtycke eller om behandlingen av olika anledningar kan anses nödvändig, exempelvis för att ge någon vård eller behandling. Också inom ramen för etikgodkänd forskning kan känsliga personuppgifter få behandlas.

[13] Se t.ex. Datainspektionens beslut 2005-09-20 (dnr 763-2005) och 2008-05-30 (dnr 390-2008).
[14] Öman och Lindblom, Personuppgiftslagen, en kommentar (4 uppl. 2011), s. 243.

Personuppgiftslagen ska inte tillämpas om det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet eller om tillämpningen skulle inskränka offentlighetsprincipen. I princip ska lagen inte heller tillämpas vid journalistisk, konstnärlig eller litterär verksamhet.

Behandling av personuppgifter ska som huvudregel anmälas till en tillsynsmyndighet.[15] Det är Datainspektionen som är denna tillsynsmyndighet. Om Datainspektionen i sin tillsynsverksamhet konstaterar att personuppgifter behandlas på ett felaktigt sätt kan myndigheten vid vite förbjuda en fortsatt behandling, eller förelägga den behandlande att vidta rättelse. Datainspektionens tillsynsansvar beskrivs närmare i redovisningen av utredningens kartläggningsarbete i kapitel 6.

Personuppgiftslagen grundar sig på ett EU-direktiv, 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, ofta kallad dataskyddsdirektivet. Direktivet liksom de beslutade nya EU-rättsakterna på dataskyddsområdet, beskrivs ytterligare nedan. Den nya dataskyddsförordningen medför bland annat att personuppgiftslagen måste upphävas.

Personuppgiftslagen kompletteras av en stor mängd s.k. registerförfattningar, som reglerar register och andra personuppgiftssamlingar i den offentliga sektorn. Syftet med registerförfattningarna är att ge ett anpassat skydd för den personliga integriteten vid vissa myndigheters personuppgiftsbehandling, där det ansetts föreligga ett behov av att avvika från eller komplettera personuppgiftslagens skydd. Detta gäller exempelvis vid särskilt känsliga register. Exempel på särskilda registerförfattningar är polisdatalagen (2010:361), domstolsdatalagen (2015:728) och patientdatalagen (2008:355) samt ett stort antal lagar om behandling av personuppgifter i särskilt angivna verksamheter, såsom lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet och lagen (2002:546) om behandling av personuppgifter inom den

[15] Det finns emellertid många undantag från anmälningsskyldigheten. En anmälan behöver t.ex. inte göras om det finns ett personuppgiftsombud eller om något av undantagen som regeringen föreskrivit i personuppgiftsförordningen(1998:1191) är tillämpligt.

arbetsmarknadspolitiska verksamheten. Också sådan särskild registerlagstiftning påverkas av EU:s reform på dataskyddsområdet.

Informationshanteringsutredningen har i sitt slutbetänkande Myndighetsdatalag (SOU 2015:39) föreslagit att personuppgiftslagen på myndighetsområdet ersätts med en ny lag, en myndighetsdatalag, som ska innehålla bestämmelser som kan gälla generellt för personuppgiftsbehandling vid alla statliga och kommunala myndigheter, med undantag för myndigheterna inom den brottsbekämpande sektorn. Förslaget har varit föremål för remissbehandling och bereds inom Regeringskansliet.

Övrig svensk lagstiftning

Utöver personuppgiftslagen och registerförfattningarna finns i svensk lag också bestämmelser i annan lagstiftning som syftar till att skydda den personliga integriteten.

I brottsbalken (BrB) finns bland annat bestämmelserna i 4 kap. om brott mot frihet och frid såsom hemfridsbrott, olaga intrång och brytande av post- eller telehemlighet samt bestämmelserna i 5 kap. om förtal och förolämpning. Även 3 kap. om brott mot liv och hälsa samt 6 kap. om sexualbrotten innehåller regler som kan sägas utgöra ett skydd för den personliga integriteten i vid mening.

Sedan den 1 juli 2013 gäller enligt 4 kap. 6 a § BrB att den som olovligen med tekniskt hjälpmedel i hemlighet tar upp bilder av någon som befinner sig inomhus i en bostad eller på en toalett, i ett omklädningsrum eller ett annat liknande utrymme kan dömas för kränkande fotografering. Ansvar ska inte utdömas om gärningen med hänsyn till syftet och övriga omständigheter är försvarlig. Av förarbetena till bestämmelsen framgår att exempel på försvarlig fotografering kan vara fotografering som ett led i nyhetsförmedling, t.ex. för publicering i ett grundlagsskyddat medium, eller fotografering i syfte att dokumentera bevisning om ett brott (prop. 2012/13:69 s. 30 f.). Det är inte ett brott om bildupptagningen sker som ett led i en myndighets verksamhet.

Sedan den 1 juli 2013 gäller också kameraövervakningslagen (2013:460), som då ersatte den tidigare lagen (1998:150) om allmän kameraövervakning. Lagen ska tillgodose behovet av kameraöver-

vakning för berättigade ändamål samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten.

Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten har som ovan nämnts bland annat föreslagit att det införs en ny straffbestämmelse om olaga integritetsintrång i 4 kap. BrB. Bestämmelsen tar sikte på gärningar som innebär exempelvis att någon gör intrång i en annan persons privatliv genom att sprida bilder eller andra uppgifter om sexualliv, hälsotillstånd eller om att denne har utsatts för ett allvarligt brott. Också spridande av bilder på någon som är naken eller befinner sig i en mycket utsatt situation ska omfattas av straffbestämmelsen. För straffansvar krävs att spridningen varit ägnad att för den som uppgifterna rör innebära en kännbar skada för privatlivet och den personliga interiteten.[16]

I OSL finns många bestämmelser om sekretess för uppgifter om enskildas personliga förhållanden. Ett av syftena med dessa är att hindra att den enskildes personliga integritet kränks genom att personliga och kanske känsliga uppgifter sprids. Som exempel kan nämnas bestämmelser om sekretess för uppgifter om den enskildes personliga förhållanden i verksamhet som avser folkbokföring (22 kap.), hälso- och sjukvård (25 kap.) och brottsbekämpning (35 kap.)

Av 21 kap. 7 § OSL följer vidare att sekretess gäller för en personuppgift, om det kan antas att utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Denna bestämmelse tar, till skillnad från vad som annars är vanligast i OSL, alltså inte sikte på uppgiften som sådan utan på vad mottagaren tänker göra med den, och avser att ge ett skydd mot otillåten behandling av personuppgifter.

OSL gäller för myndigheter samt för riksdagen och kommunala beslutande församlingar. Den gäller också i vissa fall för enskilda, exempelvis en person som i sin anställning vid en myndighet har fått del av en sekretessbelagd uppgift för myndighetens räkning och för ett enskilt organ som med stöd av lag förvarar allmänna handlingar. Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt.

[16] SOU 2016:7, s. 282 f.

Den som har blivit utsatt för en otillåten personuppgiftsbehandling kan ha rätt till skadestånd. Den personuppgiftsansvarige ska enligt 48 § personuppgiftslagen ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen har orsakat. Det krävs inte att den personuppgiftsansvarige har haft för avsikt att skada den registrerade, eller ens att han eller hon har varit slarvig, utan skadeståndsansvaret uppkommer så snart bestämmelserna i lagen har åsidosatts. Bara om den personuppgiftsansvarige kan visa att felet inte berodde på honom eller henne finns det en möjlighet att genom jämkning minska eller helt ta bort skadeståndsskyldigheten. När den personuppgiftsansvarige är en statlig myndighet kan den enskilde få sitt skadeståndsanspråk prövat av Justitiekanslern som i förekommande fall ålägger den felande myndigheten att utge ersättning. Säkerhets- och integritetsskyddsnämnden (SIN), som utövar tillsyn över bland annat behandling av personuppgifter inom polisens brottsbekämpande verksamhet, har en särskilt reglerad skyldighet att till Justitiekanslern anmäla felaktigheter som nämnden har uppmärksammat i sin tillsyn som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person.[17] En motsvarande anmälningsskyldighet har Statens inspektion för försvarsunderrättelseverksamheten (Siun).[18]

3.2.4 Dataskyddsdirektivet och EU:s dataskyddsreform

Personuppgiftslagen grundar sig som nämnts på det s.k. dataskyddsdirektivet. Syftet med direktivet är dels att skapa en hög och likvärdig skyddsnivå i alla medlemsstater när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, dels att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Direktivet gäller bara behandling av personuppgifter om fysiska personer och inte på områden som faller utanför unionsrätten, såsom försvar och allmän säkerhet. Det finns också andra rättsakter som kompletterar dataskyddsdirek-

[17] 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.
[18] 15 § förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten.

tivet, bland annat rådets rambeslut 2008/977/RIF av den 27 november 2009 om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, det s.k. dataskyddsrambeslutet.

Dataskyddsdirektivet har genomförts i medlemsstaterna genom nationell lagstiftning – i Sverige alltså genom främst personuppgiftslagen – och medlemsstaterna får inom direktivets ram precisera villkoren för personuppgiftsbehandling. De nationella preciseringarna får dock inte hindra det fria flödet av personuppgifter inom EU.

Både dataskyddsdirektivet och dataskyddsrambeslutet har varit föremål för ett omfattande reformarbete inom EU, i syfte att ytterligare harmonisera och effektivisera skyddet av personuppgifter. EU-förhandlingarna har pågått sedan 2012 och i april 2016 antog rådet och parlamentet dels en dataskyddsförordning med en generell reglering som ska ersätta dataskyddsdirektivet, dels ett nytt direktiv med särskilda regler om dataskydd för den brottsbekämpande verksamheten.[19] Förordningen ska börja tillämpas i medlemsstaterna den 25 maj 2018 och direktivet ska vara implementerat senast den 6 maj 2018.

En EU-förordning är direkt tillämplig i medlemsstaterna och därför kommer dataskyddsförordningen att ersätta inte bara dataskyddsdirektivet utan även den nationella lagstiftning i medlemsstaterna som har antagits för att genomföra direktivet, dvs. i Sverige framför allt personuppgiftslagen. En särskild utredare har fått i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som förordningen ger anledning till.[20] Även registerförfattningar och annan sektorsspecifik nationell lagstiftning som berörs av dataskyddsförordningens tillämpningsområde kommer att behöva ses över. Här lämnar förordningen dock ett visst utrymme för medlemsstaterna

[19] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv (95/46/EG (allmän dataskyddsförordning) respektive Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[20] Dataskyddsutredningen (Ju 2016:04, dir. 2016:15) ska redovisa sitt uppdrag i maj 2017.

att behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av förordningen.

Ett direktiv ska genomföras i medlemsstaterna genom nationell lagstiftning. Även här har en särskild utredare utsetts, med uppdraget att föreslå hur genomförandet i svensk rätt ska ske.[21]

De nya dataskyddsrättsakterna, och vissa av de anpassningar som behöver göras i Sverige när det gäller tillsyn, behandlas vidare i kapitel 9.

3.2.5 Några andra internationella förpliktelser

Sverige är också bundet av ett flertal andra internationella överenskommelser, varav vissa utgör bindande rättsliga regler och andra har formen av rekommendationer och riktlinjer.

Av Europakonventionens artikel 8 följer att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. En genomgång av Europadomstolens praxis visar att vad som bland annat skyddas är renodlade uppgifter om en enskilds person och identitet, men också uppgifter som rör relationen till andra människor och uppgifter som rör den enskildes yrkesliv. Härutöver ska den enskilde ha rätt till skydd när det gäller angrepp mot ”ära och ryktbarhet”.[22] Behandling av personuppgifter omfattas av artikeln, om denna avser uppgifter om den enskildes privatliv, familjeliv, hem eller korrespondens. En inskränkning i dessa rättigheter får bara göras med stöd av lag och om det är nödvändigt med hänsyn till de ändamål som är angivna i artikeln.

Sverige har tillträtt Europakonventionen, och den gäller sedan 1995 också som lag i Sverige. Enligt 2 kap. 19 § regeringsformen får en lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Europeiska unionens stadga om de grundläggande rättigheterna är genom Lissabonfördraget rättsligt bindande i alla medlemsstater. Stadgan gäller den verksamhet som utförs av EU:s organ och institutioner och den blir tillämplig för medlemsstaterna när de tillämpar EU-rätten. Av stadgans artikel 7 följer att var och en har

[21] Utredningen om 2016 års dataskyddsdirektiv (2016:06, dir. 2016:21) ska i ett delbetänkande i april 2017 redovisa vissa frågor och senast i september 2017 slutredovisa uppdraget.
[22] Se t.ex. K.U. mot Finland, nr 2872/02, och von Hannover mot Tyskland, nr 59320/00.

rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. I artikel 8 föreskrivs vidare att var och en har rätt till skydd för de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt och för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har vidare rätt att få tillgång till de insamlade uppgifter som rör honom eller henne och att få rättelse av dem.

Härutöver skyddas den personliga integriteten i bland annat Europarådets dataskyddskonvention, Förenta Nationernas allmänna förklaring om de mänskliga rättigheterna och i dess konvention om medborgerliga och politiska rättigheter, samt i riktlinjer utarbetade inom OECD. Det finns, inte minst inom EU, dessutom ett flertal sektorsspecifika rättsakter som syftar till att skydda den enskildes personliga integritet. En sådan är det s.k. e-privacydirektivet.[23]

[23] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

4 Tillsyn

4.1 Tillsynsbegreppet

Intresset för tillsyn som förvaltningspolitiskt instrument växte på allvar fram under 1990-talet och har sedan dess legat på en hög nivå. Till stor del torde det stora intresset sammanhänga med de förvaltningspolitiska förändringar som har skett under de senaste decennierna. Dessa kan sammanfattas med termer som renodling, avreglering, bolagisering, decentralisering och privatisering. Det har producerats ett stort antal studier, granskningar och utvärderingar om tillsyn. Här kan nämnas Tillsynsutredningens betänkanden Statlig tillsyn – Granskning på medborgarnas uppdrag (SOU 2002:14) och Tillsyn. Förslag om en tydligare och effektivare tillsyn (SOU 2004:100). Statskontoret har i ett stort antal publikationer behandlat tillsyn ur olika aspekter, t.ex. i studien Tänk till om tillsynen – Om utformningen av statlig tillsyn, 2012. Även inom forskningsvärlden har tillsynen granskats och studerats.

Tillsyn kan ha många former och syfta till att kontrollera olika saker, såsom resultat, effektivitet och regelefterlevnad. Tillsyn är ett av många instrument i statsförvaltningen, ett sätt för riksdagen och regeringen att försäkra sig om att den beslutade politiken och de övergripande målen för en viss verksamhet genomförs och uppnås i praktiken. Tillsyn utgör en kontroll i efterhand av hur en verksamhet fungerar, men kan också sägas ha en framåtblickande funktion eftersom de iakttagelser och erfarenheter som tillsynen ger upphov till kan användas som grund för planering, förbättring och effektivisering både av den granskade verksamheten och av andra verksamheter där liknande frågeställningar är aktuella.

Tillsyn kan därigenom vara ett verktyg för att se till att demokratiskt fattade beslut genomförs på det sätt som var avsett. Tillsynen ska bidra till att medborgarnas rättssäkerhet garanteras

samt till att respekten för folkviljan och förtroendet för staten upprätthålls. Härutöver kan tillsynen syfta till att säkerställa att den granskade verksamheten bedrivs effektivt och att konkurrerande verksamheter kan bedrivas på lika villkor. Bristande tillsyn kan leda till ett minskat förtroende för demokratiskt fattade beslut.

Tillsyn kan uppfattas som synonymt med begrepp som uppföljning, utvärdering och revision, men även om också dessa verksamheter innebär någon form av efterhandsgranskning, har de typiskt sett något olika innebörd. Uppföljning och utvärdering har det gemensamt att de, till skillnad från tillsyn, inte behöver vara och ofta inte heller är styrda av lagar och andra föreskrifter utan ofta är en frivillig efterhandsgranskning för att exempelvis dra lärdom av tidigare erfarenheter för att utveckla verksamheten. Vad som undersöks behöver heller inte vara formell regelefterlevnad eller i vilken utsträckning ärenden handlagts på ett resurseffektivt sätt, utan i stället exempelvis vilka effekter en viss bestämmelse har fått eller om målen med en verksamhet har uppnåtts. Statskontoret har definierat utvärdering som en systematiskt genomförd undersökning för att få fram tillförlitliga och användbara resultat om värdet eller förtjänsterna av en given aktivitet i ett givet sammanhang.[1] Medan uppföljning ofta beskriver enbart utfallet av en insats, innebär utvärdering alltså också en bedömning av effekterna av insatsen, dvs. om utfallet är orsakat av insatsen.

Den huvudsakliga skillnaden mellan tillsyn och utvärdering blir därmed att bedömningskriterierna vid tillsyn alltid är relaterade till relevanta lagar och andra föreskrifter, medan kriterierna vid utvärdering kan variera och vara beroende av vad utvärderaren är intresserad av att få veta.

Tillsyn behöver emellertid inte avse handläggningen av enskilda ärenden efter exempelvis klagomål, utan kan också bestå i s.k. systemtillsyn, som granskar exempelvis en myndighets organisation och processer att hantera vissa uppgifter. Så kan t.ex. en systemtillsyn avse om en myndighet har tillförlitliga system – såsom kompetensutveckling för personalen eller en organisation som kan hantera variationer i tillströmningen av ärenden – för att

[1] Utvärdera för ett bättre beslut! Att beställa utvärderingar som är till nytta i beslutsfattandet. Statskontorets rapport 2001:22.

säkerställa att dess beslut fattas i enlighet med lagar och andra föreskrifter och utan onödigt dröjsmål.

Revision å sin sida är ofta en reglerad granskning, som har sitt huvudsakliga fokus på frågan om verksamhetens resultat i förhållande till insatta resurser.

Även möjligheten att överklaga ett beslut kan beskrivas som en form av tillsyn, eftersom det innebär att en högre instans kan ”granska” underinstansens handläggning och tillämpning av gällande föreskrifter. Tillsyn är dock ett betydligt vidare begrepp, som kan omfatta kontroll av mer än överklagbara beslut vid myndigheter eller domstolar.[2]

Utgångspunkten för oss är i denna utredning den definition av begreppet tillsyn som slagits fast av regeringen i den s.k. tillsynsskrivelsen.[3] Begreppet tillsyn bör enligt denna definition användas för ”verksamhet som avser självständig granskning för att kontrollera om tillsynsobjekt uppfyller krav som följer av lagar och andra bindande föreskrifter och vid behov kan leda till beslut om åtgärder som syftar till att åstadkomma rättelse av den objektansvarige.” Ibland kan, med hänsyn till förhållandena inom ett visst tillsynsområde, avsteg från denna definition enligt regeringen behöva göras. Sådana avsteg kan vara motiverade om det leder till en mer ändamålsenlig tillsyn. Det går enligt regeringen inte att bortse ifrån att många tillsynsområden har väsentligt olika förutsättningar.[4]

4.2 Olika typer av offentlig tillsyn

Frågan om variationer i den statliga tillsynsverksamheten berördes bland annat i den förvaltningspolitiska propositionen (prop. 2009/10:175 s. 95 f.). Regeringen konstaterar där att dagens statliga tillsyn består av många skilda verksamheter och att en stor mängd statliga myndigheter har tillsynsuppgifter. Den offentliga

[2] En annan sak är givetvis att ett beslut i ett tillsynsärende kan vara möjligt att överklaga. Så kan exempelvis tillsynsbeslut meddelade av Datainspektionen eller Post- och telestyrelsen överklagas till allmän förvaltningsdomstol.
[3] Skr. 2009/10:79 En tydlig, rättssäker och effektiv tillsyn. Riksdagen har ställt sig bakom skrivelsen (bet. 2009/10:FiU12, rskr. 2009/10:210). Även enligt 2010 år förvaltningspolitiska proposition ska skrivelsen vara vägledande för det fortsatta arbetet på tillsynsområdet (prop. 2009/10:175 s. 96).
[4] A. skr. 2009/10:79 s. 13.

tillsynen har utvecklats parallellt inom de många områden där den utförs. Definitioner, synsätt, lagstiftning, praxis och förhållningssätt har vuxit fram inom respektive område. De stora variationerna i tillsynens utformning och tillämpning kan enligt regeringen i vissa fall vara en tillgång, eftersom de skapar flexibilitet. Samtidigt kan variationerna göra att tillsynsinstrumentet blir svårtillämpat och otydligt.

När tillsyn över offentlig verksamhet diskuteras är det i regel s.k. extern tillsyn som avses, dvs. tillsyn som utförs av ett annat organ än den vars verksamhet ska granskas. Detta gäller inte minst i sammanhang när tillsynens betydelse för att stärka förtroendet för verksamheten diskuteras. Men även intern tillsyn fyller en viktig funktion. Den som utför tillsynen har då framförallt en god kunskap både om den verksamhet som ska kontrolleras och de särskilda risker denna verksamhet kan innebära. Intern tillsyn är vidare normalt mindre kostsam och enklare att genomföra, och den innebär ofta färre verksamhetsstörande inslag, såsom att ta emot tjänstemän från den externa tillsynsmyndigheten och ställa samman det material som för tillsynen. Det kan också hävdas att om brister upptäcks under en intern tillsyn kan förändringsförslag ha bättre förutsättningar att få genomslag i praktiken eftersom de bygger på en god kännedom om den aktuella verksamheten och kanske till och med är förankrade i förväg. Det anförs emellertid ofta att extern tillsyn inger ett större förtroende hos allmänheten, eftersom det organisatoriska oberoendet kan uppfattas som en garanti för en större opartiskhet. De rollkonflikter som kan uppkomma inom en verksamhet vid intern kontroll har också ansetts vara något som bör undvikas.[5] Fördelar och nackdelar med intern respektive extern tillsyn torde kunna variera beroende av vilken verksamhet som ska granskas.

Tillsyn kan vara ordinär eller extraordinär. Ordinär tillsyn utövas av ett organ som i regel har som sin huvudsakliga uppgift att utöva kontroll över en viss verksamhet. Exempel på sådana organ är några av de myndigheter som är aktuella i denna utredning, såsom Datainspektionen och Post- och telestyrelsen. Ett ordinärt tillsynsorgan kan ha befogenheter att, med respekt för myndigheters själv-

[5] Prop. 2009/10:175 Offentlig förvaltning för demokrati, delaktighet och tillväxt, s. 72 f. samt skr. 2013/14:155 Regeringens förvaltningspolitik, s. 26.

ständighet enligt 12 kap. 2 § regeringsformen, ingripa i handläggningen av ärenden vid ett tillsynsobjekt, ändra fattade beslut och besluta om sanktioner. Extraordinär tillsyn utövas av Riksdagens ombudsmän (Justitieombudsmannen, JO) och Justitiekanslern (JK), som saknar dessa befogenheter. Dessa myndigheters beslut i tillsynsärenden saknar därmed rättslig verkan och utgör enbart vägledande och ibland kritiska uttalanden. Uttalanden av Justitieombudsmannen och Justitiekanslern åtnjuter emellertid av tradition en sådan respekt i den offentliga verksamheten att de kan sägas vara bindande i praktiken. Ordinär och extraordinär tillsyn kan avse samma tillsynsobjekt och samma frågeställning.

Ordinära tillsynsmyndigheters s.k. ingripande- eller sanktionsmöjligheter varierar också. Inom vissa områden finns ingen annan egentlig sanktion utöver tillsynsmyndighetens möjlighet att vid upptäckta felaktigheter uttala kritik eller anmärkningar mot den granskade verksamheten. I andra fall kan tillsynsmyndigheten vid olika typer av brister exempelvis kräva rättelse, dra in ett tillstånd, förelägga vite, besluta om straffavgifter eller förbjuda fortsatt verksamhet. En konstaterad brist kan också gälla en straffsanktionerad föreskrift och i sådana fall åligger det ofta tillsynsmyndigheten att anmäla bristen till polis och åklagare.

Det är inte ovanligt att en tillsynsmyndighet samtidigt har uppgifter som snarare är främjande, normerande eller tillståndsgivande. Det finns också tillsynsmyndigheter som ger råd i enskilda fall. Tillsynsutredningen identifierade åtta olika modeller för kombinationen av reglering, råd och tillståndsgivning hos tillståndsmyndigheter, från tillsyn utan kompletterande föreskriftsrätt eller rådgivning (t.ex. bilprovningen) till en tillsyn som kompletteras med alla övriga funktioner (t.ex. inom livsmedelskontrollen).[6]

Statskontoret, 2006 års förvaltningskommitté, Riksdagens revisorer m.fl. har pekat på problem med att en tillsynsmyndighet också har främjande, normerande eller tillståndsgivande funktioner. Det kan uppstå rollkonflikter om exempelvis en och samma myndighet både ska främja en verksamhet för att den ska uppnå satta mål, och i efterhand granska om målen har uppnåtts. Rollkonflikter av detta slag riskerar att skada förtroendet för granskningsverk-

[6] Tillsynsutredningens delbetänkande Statlig tillsyn – Granskning på medborgarnas uppdrag (SOU 2002:14) s. 65.

samheten, då objektiviteten i granskningen kan ifrågasättas. Det är enligt Statskontoret direkt olämpligt att en tillsynsmyndighet också beslutar om olika typer av statsbidrag.[7]

2006 års förvaltningskommitté hade i uppdrag att se över den statliga förvaltningens uppgifter och organisation. I sitt slutbetänkande Styra och ställa – förslag till en effektivare statsförvaltning (SOU 2008:118) anförde kommittén bland annat att tillsyn är en av statens grundfunktioner. En oberoende och förtroendeskapande tillsyn kräver att tillsynsmyndigheten inte har andra uppgifter som kan ge upphov till rollkonflikter. Förvaltningskommittén ansåg att länsstyrelserna utgör en lämplig bas för att åstadkomma en oberoende och självständig statlig tillsyn. Myndighetsstrukturen på regional nivå skulle därigenom kunna förenklas och effektiviseras. Bara sådan tillsyn som kräver högt specialiserad kompetens bör enligt kommittén utföras av separata tillsynsmyndigheter (bet. s. 152 f.).

I det här sammanhanget bör också Sveriges ökade internationella samarbete uppmärksammas, särskilt frågan om vad EU-medlemskapet har inneburit för svensk statlig tillsyn. I den mån det finns gemenskapsrättsliga regleringar på ett område kan dessa innebära krav på nationella organ för tillsyn. För att EU-rättsliga bestämmelser om exempelvis begränsningar i användningen av kemikalier eller regler på finansmarknadsområdet ska fungera krävs att varje medlemsstat kontrollerar att företag och andra följer reglerna. Därför måste medlemsstaterna ha fungerande och liknande system för tillsyn och sanktioner. Ibland ska denna tillsyn dessutom kombineras och samordnas med en tillsyn som utförs av ett EU-organ. Vidare kan unionen genom kommissionen sägas ha tillsyn över medlemsstaternas sätt att utöva en tillsynsuppgift, om denna följer av EU-lagstiftning.[8]

Utvecklingen inom EU går mot en ökad harmonisering av medlemsstaternas tillsyn. Detta gäller inom många områden, exempelvis finansmarknads- och miljöområdet, men i högsta grad också när det gäller skyddet för den personliga integriteten vid behandling av

[7] Se t.ex. Riksdagens revisorer (1994/95:RRV9), SOU 2008:118 (bilagedelen) och Statskontorets rapport Tänk till om tillsyn – om utformningen av statlig tillsyn (2012), s. 9 f.

[8] Frågan om EU-medlemskapets betydelse för svensk statlig tillsyn har varit föremål för kartläggning och analys av Statskontoret i studien En till syn på tillsyn – hur svenska tillsynsmyndigheter påverkas av EU, på uppdrag av Tillsynsutredningen (se SOU 2002:14). Sedan studien genomfördes torde utvecklingen mot en ökad gemensam syn på tillsyn ha ökat ytterligare.

personuppgifter. Frågan om EU:s reformarbete beträffande dataskydd och vilken betydelse detta får för nationella tillsynsmyndigheter beskrivs närmare i kapitel 9.

5 Några tidigare och pågående utredningar på integritetsskyddsområdet

5.1 Inledning

Ett antal utredningar under det senaste decenniet har på olika sätt berört frågor om skyddet för den personliga integriteten, några med särskild koppling till frågan om integritetsskyddet vid behandling av personuppgifter. Inte minst under det senaste året har flera olika utredningsdirektiv på detta område beslutats, många med kopplingar till det anpassningsarbete som är nödvändigt med anledning av EU:s dataskyddsreform.

Vi beskriver några av dessa utredningar i detta kapitel, men vill tillägga att det härutöver finns ytterligare utredningar som på ett eller annat sätt berör frågor om personlig integritet. Det stora antalet utredningar, dessutom inom olika departements ansvarsområden, innebär att behovet av samordning inom Regeringskansliet ökar. Utan tillräcklig samordning finns det en uppenbar risk att förlora överblick och helhetssyn i det pågående lagstiftningsarbetet.

5.2 Integritetsskyddskommittén och Grundlagsutredningen

Integritetsskyddskommittén genomförde en omfattande kartläggning och analys av sådan lagstiftning som rör den personliga integriteten. I delbetänkandet Skyddet för den personliga integriteten – Kartläggning och analys (SOU 2007:22) presenterades regelverket inom en mängd olika områden, tillsammans med

kommitténs bedömning av rättsläget utifrån ett integritetsskyddsperspektiv. I en sammanfattande bedömning anförde kommittén bland annat att de teknikrelaterade riskerna för integritetskränkningar i dagens samhälle är mångfalt större än förr, samtidigt som det även sker en teknisk utveckling för att förhindra eller begränsa skadeverkningarna.

Vad kommittén fann påfallande var att lagstiftaren inte har någon samlad kontroll över utvecklingen, och därmed också begränsade möjligheter att vidta åtgärder när sådana behövs liksom att bedöma i vad mån en ny företeelse som tycks utgöra ett hot mot privatlivets skydd trots allt bejakas av allmänheten. Datainspektionen riskerar enligt kommittén att i sin övervakning av regelefterlevnaden alltför mycket fastna i detaljkontroll och fjärma sig från vad medborgarna finner angeläget och oroar sig för. Det vore därför önskvärt om det kunde skapas förutsättningar för Datainspektionen att inom sitt område uppfattas mera som en allmänhetens ombudsman än vad som är fallet i dag.

I sitt slutbetänkande Skyddet för den personliga integriteten – Bedömningar och förslag (SOU 2008:3) anförde kommittén att Datainspektionens uppdrag borde breddas och utvecklas, så att myndigheten bland annat ges i uppdrag att uppmärksamma de teknikrelaterade riskerna för kränkningar av den personliga integriteten, framför allt med hänsyn till teknikens tillämpning i människors vardag. I detta arbete borde Datainspektionen samverka med de myndigheter och andra organ som har övergripande ansvar för konsumentskydd.

Kommittén menade också att det finns en brist på systemtänkande och helhetssyn i lagstiftningsarbetet som, särskilt med den rådande snabba lagstiftningstakten, riskerar att leda till att överblicken går förlorad. Kommittén ansåg därför att mycket talade för inrättandet av ett integritetsskyddsråd, med uppgift att vaka över integritetsskyddet i dess helhet. Frågan om inrättandet av ett sådant råd borde hållas levande och aktualiseras på nytt om det skulle visa sig behövas även efter den översyn av Datainspektionens roll som kommittén också föreslog.

Härutöver konstaterade kommittén att det var en brist att det på grundlagsnivå saknades bestämmelser om skydd för den personliga integriteten som på ett mer påtagligt sätt balanserade övriga i regeringsformen angivna fri- och rättigheter. Lagstiftaren borde,

ansåg man, tydligare erkänna den självständiga betydelsen av rätten till personlig integritet. En svag förankring av skyddet för den personliga integriteten i grundlagen kunde enligt kommittén innebära att integritetsskyddsaspekterna inte ges tillräcklig vikt när ny lagstiftning arbetas fram och står dessutom i kontrast till den uppfattning som kommer till uttryck i Europakonventionen, där rätten till respekt för privat- och familjelivet har en med andra grundläggande fri- och rättigheter jämbördig ställning. Mot denna bakgrund föreslog kommittén ett utvidgat materiellt grundlagsskydd för den personliga integriteten genom en begränsning av möjligheterna till betydande intrång i den personliga integriteten som sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Kommittén lämnade också förslag på en ny straffbestämmelse, som efter vissa justeringar har kommit att bli bestämmelsen om kränkande fotografering i 4 kap. 6 a BrB, och på en skyldighet för regeringen att årligen lämna information till riksdagen om utvecklingen på integritetsskyddsområdet.[1]

Grundlagsutredningen delade Integritetsskyddskommitténs bedömning att det var angeläget att grundlagsskyddet för den personliga integriteten förstärktes och att ett skydd för den personliga integriteten i linje med kommitténs förslag borde införas i regeringsformen. Utredningen lämnade därmed förslag på den bestämmelse som efter viss justering av den närmare utformningen i dag finns i 2 kap. 6 § andra stycket regeringsformen.[2]

5.3 Datalagringsutredningen

Datalgagringsutredningen, som lämnade sitt slutbetänkande Datalagring och integritet (SOU 2015:31) i mars 2015, hade bland annat i uppdrag att föreslå eventuella förstärkningar av den personliga integriteten i förhållande till lagen (2003:389) om elektronisk kommunikation. Härutöver skulle utredningen bland annat kartlägga och utvärdera hur lagen (2012:278) om inhämtning av upp-

[1] Frågan om en sådan rapporteringsskyldighet behandlas också i Integritetskommitténs delbetänkande Hur står det till med den personliga interiteten? (SOU 2016:41), se nedan och i kapitel 10.
[2] SOU 2008:125, s. 469 f., prop. 2009/10:80, bet. 2009/10:KU19.

gifter om elektronisk kommunikation i de brottsbekämpade myndigheternas underrättelseverksamhet (inhämtningslagen) har tillämpats och om det finns behov av några förändringar för att stärka rättssäkerheten eller skyddet av den personliga integriteten.[3] Bakgrunden till uppdraget var att EU-domstolen i april 2014[4] slog fast att det s.k. datalagringsdirektivet[5] var ogiltigt. Domstolen konstaterade att direktivet innebar ett omfattande och särskilt allvarligt intrång i rätten till privatliv och i skyddet av personuppgifter. Lagring av trafikuppgifter var enligt domstolen i och för sig en ändamålsenlig åtgärd för att uppnå syftet att bekämpa allvarlig brottslighet och upprätthålla allmän säkerhet. Direktivet fastställde dock inte tydliga och preciserade regler för omfattningen av intrånget i de aktuella rättigheterna, varför intrången enligt domstolen inte begränsades till vad som var absolut nödvändigt för att uppnå sitt syfte.

Utredningen fann att svensk rätt i huvudsak innehåller det skydd för den personliga integriteten som datalagringsdirektivet enligt EU-domstolen saknar. Så omfattar exempelvis lagringsskyldigheten i svensk rätt enligt utredningen inte annat än vad som är strikt nödvändigt för att uppnå syftet med regleringen, dvs. att utgöra ett led i den brottsbekämpande verksamheten. Det behövs därför enligt utredningen ingen förändring i fråga om vilka uppgiftskategorier som ska lagras. Vidare fann utredningen att det svenska regelverket är utformat på ett sådant sätt att Post- och telestyrelsen har möjlighet att bedriva en aktiv och ändamålsenlig tillsynsverksamhet även gentemot leverantörer som väljer att lagra uppgifter utanför EU. Personuppgifter får dessutom bara föras över till ett land utanför EU om landet i fråga säkerställer en adekvat nivå att skydd för uppgifterna. Utredningen ansåg därför att den oberoende myndighetskontrollen är garanterad i svensk rätt och att det inte behövs ett förbud mot att uppgifter som lagras

[3] Dir. 2014:101.
[4] Dom den 8 april 2014 i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., angående giltigheten av datalagringsdirektivet.
[5] Europaparlamentets och rådets direktiv 2006/24/EG om lagring av trafikuppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

enligt de svenska datalagringsreglerna förs över till tredje land för lagring där. [6]

Utredningen föreslår, i syfte att stärka kontrollen över de brottsbekämpande myndigheternas tillämpning av reglerna om inhämtning av abonnemangsuppgifter, bland annat att endast vissa utpekade befattningshavare inom den berörda myndigheten ska få fatta beslut om inhämtning. Vidare föreslår utredningen att uppgifter om kommunikation som i efterhand visar sig omfattas av tystnadsplikt ska förstöras.

Kartläggningen av tillämpningen av inhämtningslagen visade enligt utredningen att denna hanteras på ett i allt väsentligt tillfredsställande sätt, att lagen innebär beaktansvärd nytta i de brottsbekämpande myndigheternas underrättelseverksamhet men också att tillämpningen av lagen leder till integritetsintrång.

Utredningens förslag har remissbehandlats och bereds nu inom Regeringskansliet.

5.4 Informationshanteringsutredningen

Informationshanteringsutredningen hade bland annat i uppdrag att se över den s.k. registerlagstiftningen för att utreda förutsättningarna för att skapa en generell, enhetlig och helt eller delvis samlad reglering för myndigheternas behandling av personuppgifter (dir. 2014:31). De brottsbekämpande myndigheternas verksamhet ingick inte i uppdraget. Uppdraget var i huvudsak ett lagtekniskt reformarbete med inriktning på att göra nu gällande rätt beträffande dataskydd tydligare på myndighetsområdet.

Utredningen instämmer i sitt slutbetänkande Myndighetsdatalag (SOU 2015:39) i stort med den problembeskrivning som gör gällande att registerlagstiftningen är ett svåröverblickbart och fragmenterat rättsområde med bristande enhetlighet när det gäller struktur och normtekniska lösningar. Anpassningen är otillräcklig till annan lagstiftning av central betydelse för myndigheternas

[6] Vid Kammarrätten i Stockholm pågår nu ett mål om datalagring. En teleoperatör som av Post- och telestyrelsen har förelagts att lagra uppgifter enligt 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation har överklagat föreläggandet och gör gällande att det strider mot bland annat Europakonventionens bestämmelser om rätt till respekt för privat- och familjeliv, hem och korrespondens. Kammarrätten har begärt ett s.k. förhandsavgörande av EU-domstolen. Dom väntas under hösten 2016 (Mål nr 7380-14).

informationshantering, såsom tryckfrihetsförordningens bestämmelser om allmänna handlingar och offentlighets- och sekretesslagen (2009:400). Dessa problem skapar enligt utredningen osäkerhet i tillämpningen.

Mot denna bakgrund föreslår utredningen en ny lag som innehåller bestämmelser som kan gälla generellt för personuppgiftsbehandlingen vid alla statliga och kommunala myndigheter utom de brottsbekämpande. En sammanhållen lag innebär enligt utredningen ett tydligt regelverk som är lättare att tillämpa och bättre anpassat till övrig reglering av betydelse för myndigheternas informationshantering. Den ger också bättre förutsättningar för allmänhetens insyn och för enskilda registrerades möjligheter att göra gällande sina rättigheter. Till bilden hör vidare enligt utredningen att en samlad reglering är mer ändamålsenlig för att möta den förändring som förväntas ske i och med EU:s dataskyddsreform.[7]

Utredningen föreslår att tillsynsmyndigheten enligt den nya lagen ska kunna förelägga en myndighet som behandlar personuppgifter på ett felaktigt sätt att uppfylla sina skyldigheter. Vid allvarliga brister ska tillsynsmyndigheten kunna förbjuda fortsatt behandling. Den möjlighet som finns i dag för tillsynsmyndigheten att ansöka vid domstol om utplåning av olagligt behandlade uppgifter ska finnas kvar även i den nya lagen. I förebyggande syfte ska tillsynsmyndigheten härutöver genom påpekanden eller liknande förfaranden kunna avvärja eventuella brister. Någon befogenhet för tillsynsmyndigheten att besluta om vite föreslås inte.

Utredningen berörde inte särskilt frågan vilken myndighet som ska vara tillsynsmyndighet utan synes förutsätta att det är Datainspektionen som ska vara nationell tillsynsmyndighet i Sverige även enligt den nya EU-lagstiftningen och den nya lagen.

[7] En ny allmän dataskyddsförordning ska börja tillämpas den 25 maj 2018 och ett nytt dataskyddsdirektiv om behandling av personuppgifter inom det brottsbekämpande området ska vara implementerat senast den 6 maj 2018. Förordningen och direktivet beskrivs närmare i kapitel 9.

5.5 Polisorganisationskommittén

Ett av uppdragen för Polisorganisationskommittén var att utreda behovet av ett fristående organ med uppgift att granska polisens och Kriminalvårdens verksamhet. I delbetänkandet Tillsyn över polisen (SOU 2013:42) föreslog kommittén inrättandet av en fristående tillsynsmyndighet med uppgift att kontrollera att polisens verksamhet uppfyller de krav som följer av lagar och andra föreskrifter. I slutbetänkandet Tillsyn över polisen och Kriminalvården (SOU 2015:57) föreslår kommittén att den nya myndigheten ska utöva tillsyn även över Kriminalvårdens verksamhet.

I kommitténs uppdrag ingick även att analysera hur tillsynen över polisens personuppgiftsbehandling kan organiseras, så att överlappning mellan olika tillsynsmyndigheter i så stor utsträckning som möjligt undviks (dir. 2014:17). Kommittén konstaterar emellertid att regeringen sedan dess hade tillsatt vår utredning och att resultatet av detta arbete inte borde föregripas. Kommittén lämnar därför inga förslag om förändringar i Datainspektionens och Säkerhets- och integritetsskyddsnämndens nuvarande tillsynsansvar (bet. s. 67).

Kommitténs förslag har remissbehandlats och bereds för närvarande inom Regeringskansliet.

5.6 Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten

En särskild utredare har haft i uppdrag att göra en bred översyn av det straffrättsliga skyddet för enskildas personliga integritet, särskilt när det gäller hot och andra kränkningar, och att analysera om detta skydd är ändamålsenligt (dir. 2014:74). Utredningen redovisade sitt uppdrag i februari 2016 i betänkandet Integritet och straffskydd (SOU 2016:7). En stor del av analysen inriktades på hur samhällsutvecklingen och den tekniska utvecklingen har förändrat möjligheterna till kommunikation och följaktligen möjligheterna att begå sådana gärningar som innebär hot och kränkningar. Utredaren konstaterar att teknikutvecklingen, samtidigt som den innebär fördelar både för det demokratiska samhället och för individen, också innebär risker för den personliga integriteten.

Det straffrättsliga skyddet måste enligt utredaren vidgas för att vara ändamålsenligt.

Utredningen föreslår mot den bakgrunden bland annat att det införs en ny straffbestämmelse om olaga integritetsintrång. Den föreslagna bestämmelsen innebär ett straffansvar för den som gör intrång i någon annans privatliv genom att sprida bilder eller andra uppgifter på ett sätt som är ägnat att medföra kännbar skada för den som uppgiften rör. Bestämmelsen ska ta sikte endast på allvarliga och uppenbara fall av intrång i privatlivet och kränkningar av den personliga integriteten, och på intrång som består i att exempelvis sprida en bild eller annan uppgift om någons sexualliv eller hälsotillstånd eller om att någon befinner sig i en mycket utsatt situation. Straffansvaret ska enligt förslaget vara oberoende av vilken teknik för spridning som har använts, t.ex. genom internet eller annan elektronisk kommunikation, genom papperskopior eller muntligen. Utredningen har också gjort en översyn av bestämmelserna om olaga hot, ofredande, förtal och ofredande och lämnar vissa förslag om förändringar av dessa bestämmelser. Slutligen föreslår utredningen att straffansvaret enligt lagen (1998:112) om ansvar för elektroniska anslagstavlor utvidgas i några hänseenden och att rätten till brottsskadeersättning utvidgas till vissa ärekränkningsbrott.

Utredningens förslag har varit föremål för remissbehandling och bereds för närvarande inom Regeringskansliet.

5.7 Mediegrundlagskommittén

I regeringens direktiv till Mediegrundlagskommittén (dir. 2014:97 och 2016:11) konstateras bland annat att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet, vilket i praktiken innebär att personuppgiftslagens bestämmelser till skydd för den personliga integriteten inte gäller i medier som omfattas av tryckfrihetsförordningen (TF) och yttrandefrihetsgrundlagen (YGL). Vidare konstateras att var och en genom att ansöka om utgivningsbevis kan få ett sådant s.k. frivilligt grundlagsskydd för sin databas, liksom att det på senare tid har blivit allt vanligare att personuppgifter, såsom uppgifter om enskildas inkomst eller domar

i brottmål, tillhandahålls på internet av webbplatser där innehavaren har utgivningsbevis. Det kan enligt regeringen ifrågasättas om dessa webbplatser ägnar sig åt sådan massmedial verksamhet som det frivilliga grundlagsskyddet främst är avsett att skydda.

Mot denna bakgrund har kommittén bland annat haft i uppdrag att analysera vilka konflikter med skyddet för den personliga integriteten som uppkommer när information tillhandahålls ur databaser med utgivningsbevis och att ta ställning till om det behövs förändringar av regleringen för att tillgodose integritetsskyddet. Analysen ska innebära en avvägning mellan intresset av yttrandefrihet och intresset att skydda enskildas personliga integritet.

Kommittén redovisade sitt uppdrag den 15 september 2016 i betänkandet Ändrade mediegrundlagar (SOU 2016:58).

Kommittén har bland annat gjort en översyn av språket och strukturen i TF och YGL, samt övervägt frågor om grundlagsskyddet för bland annat internetpubliceringar utan koppling till traditionella medier, s.k. print on demand och e-böcker samt för databaser med användarkommentarer och länkar till andra webbsidor. Kommittén föreslår också en begränsning i en ansvarig utgivares ansvar för material i en databas som är äldre än ett år.

Av en undersökning som kommittén har låtit göra av databaser med utgivningsbevis framgår att även om de flesta verksamheter i allt väsentligt bedrivs på ett seriöst och ansvarsfullt sätt, förekommer det också att ett antal utgivningsbevis avser rena söktjänster. Som regel rör detta olika on line-tjänster vilka bedrivs på kommersiella grunder och som innebär att allmänheten ges tillgång till information om enskilda som hämtats ur offentliga handlingar och register. Verksamhet av det slaget är integritetskänslig och det är enligt kommittén uppenbart att enskilda riskerar att lida skada av att den aktuella informationen sprids till allmänheten. Behovet av att låta verksamheter av detta slag fullt ut skyddas av de tryck- och yttrandefrihetsrättsliga grundprinciperna framstår enligt kommittén som begränsat och den nuvarande situationen innebär att grundlagssystemet när det gäller dessa söktjänster riskerar att få konsekvenser som inte är rimliga. Problemet blir enligt kommittén särskilt påtagligt om den grundlagsskyddade databasen används för att behandla och tillhandahålla uppgifter som i andra sammanhang

anses särskilt känsliga, t.ex. att någon har varit tilltalad i ett brottmål.

Kommittén anser mot denna bakgrund att det finns skäl att inskränka grundlagsskyddet för vissa typer av söktjänster och i stället tillåta bestämmelser på lagnivå. Kommittén föreslår därför ett uttryckligt undantag i TF och YGL som tar sikte på vissa rena söktjänster som tillhandahåller känsliga personuppgifter och uppgifter om lagöverträdelser m.m. Samtliga uppgiftssamlingar som har ordnats så att det är möjligt att söka efter eller sammanställa de aktuella uppgifterna ska omfattas av undantaget. En förutsättning för att undantag ska gälla är att det med hänsyn till verksamheten och de former under vilka uppgiftssamlingen hålls tillgänglig finns särskilda risker för otillbörliga intrång i de registrerades personliga integritet. Det aktuella undantaget utformas enligt förslaget som en s.k. delegationsbestämmelse genom vilken det skapas utrymme att reglera frågan på annat sätt än genom grundlag.[8]

5.8 Integritetskommittén

Den parlamentariskt sammansatta Integritetskommittén (Ju 2014:09) har i uppdrag att kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet. Kartläggningen och analysen ska göras med ett individperspektiv. Kommittén ska också inom ramen för detta arbete följa upp effekterna i lagstiftningsarbetet av den förstärkning av grundlagsskyddet för den personliga integriteten som genomfördes 2011.

Regeringen konstaterar i kommitténs direktiv (dir. 2014:65) att ansvaret att tillvarata enskildas intresse av skydd för den personliga integriteten delas av en rad myndigheter men att det inte finns något enskilt statligt organ som har ett bredare och mera övergripande uppdrag att följa utvecklingen på integritetsskyddsområdet.

[8] Vid Europadomstolen för mänskliga rättigheter (Grand Chamber) prövas i september 2016 ett mål som bland annat gäller tillhandahållandet av personuppgifter (enskildas taxeringsuppgifter), huruvida ett sådant tillhandahållande är att betrakta som publicistisk verksamhet och hur en publicering av uppgifterna förhåller sig till rätten till yttrandefrihet enligt artikel 10 i Europakonventionen (Satakunnan Markkinapörssi Oy och Satamedia Oy v. Finland, mål nr 931/13).

Det finns enligt regeringen nu anledning att överväga och ta ställning till värdet och behovet av en myndighet med ett brett och samlat uppdrag att följa utvecklingen på området för den personliga integriteten. Med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna i kartläggnings- och analysuppdraget ska kommittén därför följa upp Integritetsskyddskommitténs förslag om ett integritetsskyddsråd och särskilt överväga om ett sådant råds uppgifter kan fullgöras av en befintlig myndighet.

I delbetänkandet Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén (SOU 2016:41) redovisade kommittén i juni 2016 dels kartläggningen och analysen av riskerna för integritetsintrång, dels uppdraget som gällde behovet av att inrätta ett integritetsskyddsråd.

Kommittén konstaterar att vi alla i dag för att ta del av många fördelar med den moderna informationstekniken måste dela med oss av uppgifter om oss själva och ibland om våra vänner. Det är enligt kommittén svårt att överblicka hur dessa uppgifter samlas in, sprids och vidareanvänds, och behandlingen av personuppgifter riskerar att bli närgången. För att göra det möjligt att jämföra de risker för den personliga integriteten som är förknippade med olika företeelser i samhället beskriver kommittén riskerna utifrån tre nivåer; viss risk, påtaglig risk eller allvarlig risk för den personliga integriteten. En riskbedömning utgår dels från sannolikheten för att ett intrång inträffar, dels från effekterna eller konsekvenserna av ett sådant intrång.

Företeelser som är förknippade endast med viss risk för den personliga integriteten är enligt kommittén sådana som de flesta inte blir föremål för, eller sådana där inte så många eller känsliga personuppgifter behandlas. De kan också vara reglerade genom tydlig lagstiftning. Exempel på företeelser som enligt kommittén innebär en viss risk för den personliga integriteten är hanteringen av personuppgifter inom skolornas elevhälsa, arbetsgivares granskning av vad arbetstagare skriver på sociala medier, Kronofogdemyndighetens och inkassoföretagens verksamheter samt polisens brottsbekämpande spaningsverksamhet på internet.

När det gäller företeelser som är förknippade med påtagliga risker för den personliga integriteten handlade det enligt kommittén ofta om företeelser som innefattar behandling av flera olika uppgifter om

enskilda och om behandlingar som omfattar många. De uppgifter som behandlas kan vara känsliga eller närgångna. Sådana företeelser är ofta reglerade, men har enligt kommittén ibland brister i regelverket eller i tillämpningen av dessa. Här nämns bland annat kameraövervakning inomhus i skolor, informationsdelning inom och mellan myndigheter, oskyddad e-post samt polisens behandling av personuppgifter i register.

Företeelser som enligt kommittén är förknippade med allvarliga risker för den personliga integriteten omfattar ofta stora delar av befolkningen och avser behandling av mycket känsliga eller närgångna personuppgifter. Sådana företeelser kan sakna reglering eller ha stora brister i regelverket eller i tillämpningen av dessa. Sådana företeelser är enligt kommittén bland annat kameraövervakning på arbetsplatser, hälso- och sjukvård samt välfärdstjänster inom socialtjänsten, brister i myndigheters informationssäkerhet, användningen av kreditkort och andra digitala transaktioner samt kreditupplysningsföretagens verksamhet.

Integritetskommittén föreslår att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör den personliga integriteten och ny teknik ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen. Vidare föreslår kommittén att regeringen ska lämna en årlig skrivelse till riksdagen med motsvarande information. Däremot ser kommittén inte något behov av ett nytt integritetsskyddsorgan (integritetsskyddsråd) med huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen.

Integritetskommitténs uppdrag ska slutredovisas senast den 1 juni 2017.[9]

[9] Tilläggsdirektiv till Integritetskommittén (dir. 2016:12).

5.9 Kameraövervakning – brottsbekämpning och integritetsskydd

En särskild utredare ska utreda vissa frågor om kameraövervakning (Ju 2015:14, dir. 2015:125 och 2016:54). Syftet med uppdraget är att säkerställa att kameraövervakning kan användas där det behövs för att bekämpa brott och samtidigt garantera ett starkt skydd för den personliga integriteten. Utredaren ska bland annat kartlägga och utvärdera vad kameraövervakningslagen (2013:460) har inneburit för möjligheterna till kameraövervakning och skyddet för den personliga integriteten, analysera om möjligheterna till kameraövervakning på särskilt brottsutsatta platser och andra platser med förhöjt skyddsbehov, till exempel asylboenden, medieredaktioner och lokaler som används av religiösa samfund, behöver förbättras, samt undersöka hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom till exempel kamerautrustade drönare. Genom tilläggsdirektiv har utredaren dessutom fått i uppdrag att analysera hur regleringen i kameraövervakningslagen bör anpassas till den nya EU-rättsliga dataskyddsregleringen.

Utredningen ska redovisa sitt uppdrag senast den 15 juni 2017.

5.10 Ytterligare utredningar om anpassningar med anledning av EU:s dataskyddsreform

Bara under innevarande år har ett flertal ytterligare utredningsdirektiv beslutats som rör behandling av personuppgifter och skyddet av den enskildes personliga integritet. Bakgrunden är i flera fall de anpassningar som är nödvändiga med anledning av EU:s nya allmänna dataskyddsförordning som innebär en ny generell reglering av behandling av personuppgifter, och det nya dataskyddsdirektivet om behandling av personuppgifter på det brottsbekämpande området.

Dataskyddsutredningen (Ju 2016:04) och Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) har i uppdrag att föreslå de anpassningar och författningsbestämmelser som är nödvändiga med anledning av att den nya dataskyddsförordningen och det nya dataskyddsdirektivet ska börja tillämpas respektive ska vara genomfört i svensk rätt under 2018.

Dataskyddsutredningen ska bland annat undersöka vilka kompletterande nationella föreskrifter som förordningen kräver, överväga vilka kompletterande bestämmelser om t.ex. behandling av känsliga personuppgifter och personnummer som bör införas i den generella svenska regeringen samt undersöka om det finns behov av generella bestämmelser för personuppgiftsbehandling utanför EU-rättens tillämpningsområde. Utredningen ska redovisa sitt uppdrag senast den 12 maj 2017.[10]

Utredningen om 2016 års dataskyddsdirektiv ska bland annat lämna förslag till en ny ramlagstiftning med bestämmelser om skydd för personuppgifter inom direktivets tillämpningsområde, lämna de förslag till författningsförändringar som krävs för att bedöma om direktivet ger anledning till en ny eller ändrad reglering om tillsyn samt bedöma om det finns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat från den lagstiftning som gäller för Polismyndigheten. Utredningen ska senast den 1 april 2017 i ett delbetänkande redovisa uppdraget i den del det rör ramlagstiftning och tillsyn. Uppdraget ska slutredovisas senast den 30 september 2017.[11]

De två utredningarna har uppdrag som rör tillsyn över behandling av personuppgifter med anledning av de nya europeiska rättsakterna.

Härutöver har ytterligare utredningar fått i uppdrag att härutöver föreslå kompletterande regleringar inom olika områden.

Utredningen om personuppgiftsbehandling inom utbildningsområdet (U 2016:03, dir. 2016:63) har fått i uppdrag att föreslå kompletterande regleringar för behandling av personuppgifter inom utbildningsområdet, med undantag för forskningsverksamhet. Utredaren ska bland annat undersöka vilken reglering av personuppgiftsbehandling inom utbildningsområdet som är möjlig och kan behövas utöver dataskyddsförordningen och den generella reglering som Dataskyddsutredningen kommer att föreslå, analysera om det utöver dessa regleringar finns ett behov av kompletterande regleringar för behandling av känsliga personuppgifter inom utbildningsområdet, och analysera behovet av reglering för vissa register

[10] Dir. 2016:15.
[11] Dir. 2016:21.

inom utbildningsområdet. Uppdraget ska redovisas senast den 1 juni 2017.

Ett liknande utredningsuppdrag för forskningsområdet har Utredningen om personuppgiftsbehandling för forskningsändamål (U 2016:04, dir. 2016:65). Övervägandena om behovet av anpassningar av svensk lagstiftning avser här bland annat lagen (2003:460) om etikprövning av forskning som avser människor, lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa samt lagen (1999:353) om rättspsykiatriskt forskningsregister. Uppdraget ska delredovisas senast den 1 juni 2017 och slutredovisas senast den 8 december 2017. Också på Arbetsmarknadsdepartementets område har det tillsatts en utredning om nödvändiga anpassningar. Utredningen ska redovisa sitt uppdrag senast den 31 maj 2017 (2016:B).

Utredningen om dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde (S 2016:05, dir. 2016:52) har som namnet anger i uppdrag att analysera vilka konsekvenser dataskyddsförordningen får för regleringen av sådan personuppgiftsbehandling som sker i exempelvis receptregister, hälsodataregister, läkemedelsförteckningar och register över nationella vaccinationsprogram. Uppdraget ska redovisas senast den 31 augusti 2017.

Även domstolsdatalagen (2015:728) behöver ses över med anledning av dataskyddsförordningen. En utredning har tillsatts med uppdrag att föreslå de kompletterande bestämmelser som behövs för regleringen av domstolarnas personuppgiftsbehandling (Ju 2016:G). Uppdraget ska redovisas senast den 8 maj 2017.

Också Utredningen om en ändamålsenlig reglering för biobanker (S 2016:04, dir. 2016:41) har ett uppdrag som rör behandling av personuppgifter och skyddet för den enskildes personliga integritet. Detta uppdrag ska senast den 1 maj 2017 redovisas i vissa delar och slutredovisas senast den 31 december 2017. En särskild utredare har vidare fått i uppdrag att utreda vissa anpassningar av regelverket för Rättsmedicinalverket (RMV). I uppdraget ingår bland annat att överväga möjligheten och behovet av en särskild personuppgiftsreglering för RMV och att beakta enskildas behov av skydd för den personliga integriteten. Uppdraget ska redovisas senast den 31 oktober 2017 (Ju 2016:18, dir. 2016:75).

6 Kartläggning av dagens tillsyn över personuppgiftsbehandling

6.1 Kartläggningsarbetet

Det har ingått i utredningens uppdrag att kartlägga den tillsyn över behandling av personuppgifter som i dag bedrivs av flera myndigheter. Vi har valt att uppfatta uppdraget så att kartläggningsarbetet på ett så heltäckande sätt som möjligt ska redovisa alla de myndigheter som åtminstone teoretiskt kan sägas ha ett tillsynsuppdrag som omfattar behandlingen av personuppgifter i den granskade verksamheten. Det innebär att kartläggningen omfattar inte bara myndigheter som exempelvis Datainspektionen och Säkerhets- och integritetsskyddsnämnden (SIN), som helt eller till stor del ägnar sig åt tillsyn över personuppgiftsbehandling. Några av de myndigheter som ingår i redovisningen har ett huvudsakligt tillsynsuppdrag inom helt andra områden än dataskydd och skyddet för den personliga integriteten. Ytterligare några är inte huvudsakligen tillsynsmyndigheter utan har tilldelats ett visst tillsynsansvar utöver sina andra uppgifter.

Vi har för kartläggningen ”dammsugit” lagar och förordningar som innehåller bestämmelser om personuppgiftsbehandling, för att identifiera vilken myndighet som i varje enskilt fall ansvarar för tillsynen över denna behandling, och om det förekommer regleringar som innebär att fler än en myndighet har ett tillsynsansvar över samma personuppgiftsbehandling. Utgångspunkten för kartläggningsarbetet har varit tanken att den dataskyddsreglering som följer av det nuvarande dataskyddsdirektivet och av personuppgiftslagen (1998:204) utgör en kärna i den rättsliga regleringen av den personliga integriteten vid behandlingen av personuppgifter. Datainspektionen är tillsynsmyndighet enligt direktivet och personuppgiftslagen. Härutöver finns bestämmelser om personuppgifts-

behandling i många andra författningar, och i vissa av dessa pekas alternativa eller parallella tillsynsmyndigheter ut. I urvalet av dessa övriga författningar har vi sökt efter regleringar av dataskyddsrättslig natur som på något sätt avviker från eller kompletterar personuppgiftslagens regleringar. Vi har gjort sökningar i rättsdatabaser genom att använda sökord som exempelvis ”personuppgift”, ”register” och ”tillsyn”. Ett stort antal av sökresultatet utgörs av författningar som antingen bara hänvisar till att bestämmelser om behandlingen av personuppgifter finns i personuppgiftslagen eller som innehåller en eller flera särregleringar men ingenting om tillsyn. Som exempel på sådana författningar kan nämnas aktiebolagslagen (2005:551), lagen (2001:617) om behandling av personuppgifter inom kriminalvården och studiestödsdatalagen (2009:287).

Men som redovisningen visar finns också ett antal regleringar som innebär att andra myndigheter har ett tillsynsansvar som mer eller mindre uttryckligt omfattar även behandlingen av personuppgifter. Dessa presenteras nedan, med kommentarer om i vilken mån tillsynsverksamheten i praktiken omfattar även personuppgiftsbehandling.

En svårighet med den sökmetod vi har använt är den begränsning som följer av ett nödvändigt val av sökord. Det finns åtminstone en bestämmelse som reglerar behandling av personuppgifter utan att innehålla något av de sökord som normalt kan förknippas med sådan behandling. Av 19 § marknadsföringslagen (2008:486) följer ett förbud mot s.k. obeställd reklam till fysiska personer via exempelvis e-post, ofta kallad spam. Sådana utskick av marknadsföring innebär en behandling av personuppgifter (som omfattas av Konsumentverkets tillsyn, vilket berörs ytterligare nedan) men för att just den bestämmelsen, som inte innehåller något av de ord man normalt förknippar med behandling av personuppgifter, skulle omfattas av en databassökning skulle sökorden behöva vara så oprecisa och allmänt hållna att sökresultatet skulle bli svårt eller rent av omöjligt att hantera. Vetskapen om denna bestämmelse och dess utformning gör att vi inte kan utesluta att det finns ytterligare bestämmelser som reglerar personuppgiftsbehandling och som inte har träffats av våra sökningar.

Kartläggningen tydliggör att området för behandling av personuppgifter är mycket stort. Sådan behandling förekommer i dag i stort sett överallt i samhället, i både privat och offentlig verksam-

het. Förutsättningarna för personuppgiftsbehandlingen, både de faktiska och de rättsliga, kan variera, bland annat beroende på om behandlingen utförs av enskilda eller av myndigheter och om särskilda krav ställs på skyddet av den enskildes personliga integritet i en viss verksamhet. Dessa varierande förutsättningar påverkar också hur tillsynen är organiserad.

6.2 Resultatet av kartläggningen

6.2.1 Inledning

Med utgångspunkten att den huvudsakliga, grundläggande regleringen av personuppgiftsbehandling utgörs av dataskyddsdirektivet och personuppgiftslagen, med Datainspektionen som tillsynsmyndighet, kan den samlade regleringen av behandling av personuppgifter ses som en modell med personuppgiftslagen och Datainspektionen som en kärna och ett antal cirklar utanför denna, med författningar som i olika grad reglerar tillsynen över den reglerade personuppgiftsbehandlingen.

I det följande presenteras resultatet av kartläggningen, med Datainspektionens tillsyn först (avsnitt 6.2.2). I den kategori författningar och tillsynsmyndigheter som vi placerar närmast utanför modellens mitt återfinns lagar som innehåller uttryckliga bestämmelser om personuppgiftsbehandling och där det enligt vår mening inte råder någon tvekan om att ett tillsynsansvar även över personuppgiftsbehandlingen vilar på en viss utpekad, annan myndighet (avsnitt 6.2.3). Som kontakter med myndigheterna har tydliggjort är det dock inte alltid tillsynen i praktiken omfattar den behandling av personuppgifter som förekommer i den granskade verksamheten. I nästa kategori i modellen återfinns tillsynsmyndigheter som har ett mer allmänt utformat tillsynsuppdrag eller där ett tillsynsansvar för personuppgiftsbehandling visserligen ser ut följa av lag men snarast kan sägas vara teoretiskt(avsnitt 6.2.4). Vid sidan av de ordinarie tillsynsmyndigheterna utförs även extraordinär tillsyn av Riksdagens ombudsmän och Justitiekanslern (avsnitt 6.2.5).

I detta sammanhang kan även personuppgiftsombudens arbete nämnas. En personuppgiftsansvarig kan utse ett personuppgiftsombud och anmäla detta till Datainspektionen. Ombudet har till uppgift att självständigt, men inom den aktuella verksamheten, se

till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och påpeka eventuella brister för honom eller henne. Om rättelse då inte sker av den personuppgiftsansvarige ska ombudet anmäla förhållandet till Datainspektionen. En personuppgiftsansvarig som har utsett och anmält ett personuppgiftsombud undantas från den anmälningsplikt som annars som huvudregel råder för personuppgiftsbehandling. Ett personuppgiftsombuds uppgifter utgör inte tillsyn, men kan sägas komplettera och förstärka tillsynsmyndigheternas arbete genom att öka regelefterlevnaden i de verksamheter som omfattas av tillsyn.

De olika kategorierna och tillsynsmyndigheterna beskrivs, med utgångspunkt i de olika verksamheter och rättsliga regleringar där de aktualiseras, i de följande avsnitten.

6.2.2 Dataskyddsdirektivet, personuppgiftslagen och Datainspektionen

Den grundläggande dataskyddsrättsliga regleringen, dvs. de bestämmelser som avser att skydda den enskildas personliga integritet vid personuppgiftsbehandling, utgörs i Sverige av personuppgiftslagen. Lagen grundar sig på EU:s dataskyddsdirektiv (Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter). Ett omfattande reformarbete inom EU har resulterat i en ny dataskyddsreglering, där Europaparlamentet och rådet den 27 april 2016 antog en allmän dataskyddsförordning och ett dataskyddsdirektiv för det brottsbekämpande området. Förordningen ska börja tillämpas den 25 maj 2018 och direktivet ska vara implementerat i nationell rätt senast den 6 maj 2018. Vilka anpassningar och kompletterande författningsregleringar som krävs för svensk del med anledning av de nya rättsakterna är föremål för pågående utredningsarbeten, som beräknas vara slutförda i maj respektive september 2017.[1] Även vi har haft i uppdrag att lämna vissa förslag som behövs för att en svensk tillsynsmyndighet ska kunna fullgöra de uppgifter som

[1] Dataskyddsutredningen (Ju 2016:04, dir. 2016:15) respektive Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06, dir. 2016:21).

följer av förordningen och direktivet. Våra överväganden i dessa delar redovisas i kapitel 9.

Det nu gällande dataskyddsdirektivet föreskriver att varje medlemsstat ska ha en eller flera tillsynsmyndigheter som ska övervaka tillämpningen av de nationella bestämmelser som antagits till följd av direktivet. Tillsynsmyndigheten ska ha vissa angivna uppgifter och befogenheter. I Sverige är Datainspektionen denna myndighet.[2]

Datainspektionen har det övergripande, generella ansvaret för tillsynen över behandling av personuppgifter. Tillsynsuppdraget är brett och Datainspektionen är behörig att utöva tillsyn över all personuppgiftsbehandling.[3] Tillsynen avser både sådan behandling som regleras av personuppgiftslagen och sådan som omfattas av särskilda registerlagar med avvikande eller kompletterande bestämmelser. Utformningen av Datainspektionens behörighet innebär att det inte finns några ”luckor” i tillsynen över behandlingen av personuppgifter. Det finns med andra ord inte någon personuppgiftsbehandling som inte omfattas av någon myndighets tillsynsbefogenhet; om inte någon annan myndighet utövar tillsyn kan Datainspektionen alltid göra det.

Beskrivningen i detta avsnitt av Datainspektionens uppgifter och befogenheter tar i huvudsak sikte på vad som gäller i dag, innan de nya rättsakterna har börjat tillämpas eller implementerats. EU:s dataskyddsreform innebär dock nyheter inte minst för de nationella tillsynsmyndigheterna. En närmare beskrivning av vad dessa nyheter innebär och vilka konsekvenser de får för en svensk tillsynsmyndighet ges, så långt det är möjligt och till den del det har ansetts falla inom vårt uppdrag, i kapitel 9.

Datainspektionens uppgift är enligt sin myndighetsinstruktion att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Verksamheten ska särskilt inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud. Det åligger också myndigheten att följa och beskriva utvecklingen på IT-området när det

[2] 2 a § förordningen [2007:975] med instruktion för Datainspektionen.
[3] Härutöver har några ytterligare myndigheter i uppdrag att utöva tillsyn över behandling av personuppgifter inom vissa särskilt angivna områden, vilket beskrivs nedan. Har en annan myndighet behörighet att utöva tillsyn avstår Datainspektionen normalt från tillsynsinsatser på detta område.

gäller frågor om integritet och ny teknik. Av Datainspektionens regleringsbrev för 2016 följer vidare att myndigheten ska upptäcka och förebygga hot mot den personliga integriteten och att verksamheten främst ska inriktas på områden som bedöms vara särskilt känsliga ur ett integritetsperspektiv, nya företeelser och användningsområden av teknik samt områden där risk för missbruk eller felaktig användning bedöms vara särskilt stor.

Myndighetens verksamhet styrs i dag i huvudsak av personuppgiftslagen, personuppgiftsförordningen och förordningen med myndighetens instruktion. Dessutom innehåller en mängd internationella dokument, exempelvis Europarådets dataskyddskonvention,[4] Schengenkonventionen,[5] Prümrådsbeslutet[6] och VIS-förordningen[7] bestämmelser om nationella tillsynsmyndigheter. Det är Datainspektionen som är Sveriges nationella tillsynsmyndighet även enligt dessa dokument. Datainspektionen ingår också i den s.k. Artikel 29-gruppen, den arbetsgrupp som inrättats med stöd av artikel 29 i det nuvarande dataskyddsdirektivet och som har till uppgift att se till att direktivet tillämpas enhetligt i medlemsstaterna. Gruppen ska också bland annat ge råd till kommissionen om förslag till ändringar i direktivet. När den nya dataskyddsförordningen träder i kraft kommer denna grupp att ersättas av den s.k. dataskyddsstyrelsen, the European Data Protection Board (EDPB).

Datainspektionen är också tillstånds- och tillsynsmyndighet enligt kreditupplysningslagen (1973:1173) och inkassolagen (1974:182) och ska i denna verksamhet verka för att god sed iakttas i de verksamheter som omfattas av dessa lagar. Kreditupplysningslagen ska i första hand skydda de registrerades personliga integritet, men lagen ska också bidra till en effektiv kreditupplysningsverksamhet. Inkassolagen har bestämmelser om god inkassosed, vilket bland annat innebär att den som inkassoåtgärderna riktas mot inte får

[4] Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (artikel 13).
[5] Konventionen om tillämpning av Schengenavtalet av den 14 juni 1985 (artikel 114).
[6] Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (artikel 30.5).
[7] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för visering (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (artikel 41).

utsättas för onödiga kostnader. Datainspektionens tillsyn omfattar inte inkassoverksamheter som står under Finansinspektionens tillsyn. Detta är fallet med inkassoföretag som också ägnar sig åt exempelvis kreditgivning.

Datainspektionen avgör själv när det finns anledning att inleda ett tillsynsärende. Beslutet kan grunda sig på exempelvis iakttagelser vid ett annat tillsynsärende, en beslutad tillsynsplan, ett tips från massmedia eller andra myndigheter och klagomål från enskilda. Tillsyn kan också initieras efter en anmälan från ett personuppgiftsombud. Datainspektionen tar emot klagomål från enskilda som anser att de har varit föremål för en felaktig personuppgiftsbehandling men är inte skyldig att inleda ett tillsynsärende på grund av en gjord anmälan. Alla som klagar får dock ett besked i någon form från Datainspektionen. Av de nya EU-rättsakterna kommer att följa en i viss mån ökad skyldighet att agera med anledning av ett klagomål. Tillsynsmyndigheterna ska enligt dataskyddsförordningen och det nya dataskyddsdirektivet där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den klagande om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet (artikel 57.1 f i förordningen och artikel 46.1 f i direktivet). Om tillsynsmyndigheten underlåter att behandla ett klagomål eller att inom tre månader informera den klagande om hur ärendet fortskrider ska den registrerade ha rätt till ett effektivt rättsmedel (artikel 78.2 respektive 53.2).

Tillsyn bör enligt Datainspektionens tillsynspolicy[8] inledas i bland annat följande fall:

- vid allvarliga brister i hanteringen av personuppgifter,
- om behandlingen har utförts av en myndighet, ett stort företag eller en stor förening,
- om den enskilde befinner sig i en beroendeställning till den personuppgiftsansvarige,

[8] Datainspektionens styrdokument, Tillsynspolicy avseende PUL, 2010-02-09.

- om det är fråga om en integritetskänslig behandling, stora uppgiftsmängder om en person eller behandlingar om många människor, eller
- om det är fråga om nya företeelser där det kan finnas risk för integritetsintrång och betydande brister i säkerheten för personuppgifterna.

För att kunna genomföra ett tillsynsärende har Datainspektionen rätt att få tillgång till de personuppgifter som har behandlats. Myndigheten har också rätt att få upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna behandling, och har dessutom rätt att få tillträde till lokaler som har anknytning till den aktuella personuppgiftsbehandlingen. Inspektioner kan ske genom fältinspektion, enkätinspektion, skrivbordsinspektion eller genom s.k. förenklad tillsyn. Det är möjligt att genomföra oanmälda inspektioner, men sådana är ovanliga.

Om Datainspektionen trots en begäran inte har fått tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får inspektionen förbjuda vidare behandling på annat sätt än genom lagring. Ett sådant förbud kan förenas med vite.[9] Dessutom gäller att den som uppsåtligen eller av grov oaktsamhet lämnar osanna uppgifter till Datainspektionen, liksom den som i övrigt bryter mot vissa andra angivna bestämmelser i personuppgiftslagen, kan dömas till böter eller fängelse (49 §).

Datainspektionen kan efter en avslutad utredning genom antingen ett föreläggande eller en rekommendation ange vilka åtgärder den personuppgiftsansvarige ska eller bör vidta för att komma tillrätta med eventuella felaktigheter i personuppgiftsbehandlingen. Om rättelse inte sker kan inspektionen förbjuda den personuppgiftsansvarige att fortsätta med behandlingen. Datainspektionen har också rätt att besluta om vilka säkerhetsåtgärder som måste vidtas.

[9] Staten anses dock inte utan särskild reglering kunna bli föremål för ett vitesföreläggande, varför ett sådant beslut ofta inte kan meddelas mot andra statliga myndigheter. Se t.ex. prop. 1984/85:96 s. 24 och prop. 2012/13:143 s. 66 f. I vissa författningar är det också särskilt reglerat att ett förbud inte kan förenas med vite, t.ex. 2 kap. 2 § fjärde stycket polisdatalagen (2010:361) och 9 kap. 8 § andra stycket rättegångsbalken. Frågan om en tillsynsmyndighets möjligheter att döma ut administrativa sanktionsavgifter mot myndigheter och offentliga organ med stöd av den nya dataskyddsförordningen är föremål för utredning i Dataskyddsutredningen (Ju 2016:04, dir. 2016:15).

Vid sidan av Datainspektionen arbetar som nämnts personuppgiftsombud för att behandlingen av personuppgifter inom den egna organisationen ska vara korrekt. Om ombudet anser att det har förekommit en felaktig behandling, och om den personuppgiftsansvarige inte vidtar rättelse, ska ombudet anmäla detta till Datainspektionen, som då kan inleda ett tillsynsärende och vid behov kräva åtgärder. Ett personuppgiftsombud kan begära samråd med Datainspektionen om tolkning av personuppgiftslagstiftningen.

En stor del av Datainspektionens arbete ägnas åt förebyggande arbete i form av information och vägledning till bland annat personuppgiftsansvariga och personuppgiftsombud. Myndighetens webbplats spelar här en stor roll, och ett omfattande informationsmaterial publiceras där. Vid myndigheten finns också en särskild s.k. upplysningstjänst som via telefon och e-post besvarar frågor om bland annat personuppgiftsbehandling. Varje år inkommer närmare 10 000 frågor till upplysningstjänsten. Det omfattande förebyggande och utåtriktade arbetet syftar till att personuppgiftsbehandlingen ska bli rätt från början så att behovet av ingripande åtgärder vid felaktig behandling ska minska.

Datainspektionen yttrar sig vidare över bland annat lagförslag och branschöverenskommelser, och deltar i konferenser. Företrädare för myndigheten medverkar ofta som experter i statliga utredningar. Datainspektionen samverkar också med andra myndigheter och organisationer, i syfte att åstadkomma samsyn i integritetsfrågor och sprida kunskap om integritetsrisker, utbyta information samt att klargöra gränser mellan olika myndigheters tillsynsansvar.

Datainspektionen har även tillsynsuppgifter enligt kameraövervakningslagen, vilket beskrivs nedan.

Datainspektionens tillsyn avser personuppgiftsbehandling som utförs i både enskild och offentlig verksamhet. Myndighetens beslut kan överklagas till allmän förvaltningsdomstol.

Tillsynsverksamheten vid Datainspektionen är omfattande. Tillsyn enligt personuppgiftslagen är den största ärendekategorin, vid sidan av främst ärenden enligt kreditupplysnings- och inkassolagarna. Av totalt 139 avgjorda tillsynsärenden 2015 avsåg 82 (59 %) tillsyn enligt personuppgiftslagen. Av totalt 417 inkomna klagomål från enskilda 2015 avsåg 252 (60 %) klagomål enligt personuppgiftslagen. Härutöver avser enskildas klagomål kreditupplysnings-, inkasso- och kameraövervakningsärenden.

År 2015 avgjordes 1032 ärenden med koppling till kameraövervakningslagen. Bland dessa återfinns bland annat granskningar av länsstyrelsernas beslut i tillstånds- och tillsynsärenden, överklagande av länsstyrelsers beslut om kameraövervakning samt besvarande av frågor om kameraövervakning från allmänheten och tillverkare av kamerautrustning.

6.2.3 Andra myndigheter med ett uttryckligt tillsynsansvar över personuppgiftsbehandling

Vid sidan av dataskyddsdirektivet och personuppgiftslagen finns ett stort antal lagar och förordningar som i varierande omfattning reglerar behandling av personuppgifter. Sådana bestämmelser förekommer i föreskrifter av vitt skilda slag, både sådana vars huvudsakliga syfte är att reglera just register- och personuppgiftsfrågor och sådana som främst reglerar helt andra frågor men som också innehåller vissa bestämmelser om personuppgiftsbehandling. Exempel på den första kategorin är ett stort antal lagar om behandling av personuppgifter i olika typer av verksamhet, såsom åklagardatalagen (2015:433), apoteksdatalagen (2009:367) och lagen (2001:617) om behandling av personuppgifter inom kriminalvården. Exempel på den andra kategorin är marknadsföringslagen (2008:486) och kasinolagen (1999:355).

Gemensamt för alla dessa föreskrifter är att de innehåller en eller flera bestämmelser om personuppgiftsbehandling som kompletterar eller ersätter bestämmelser i personuppgiftslagen. I allra flesta av dessa föreskrifter finns ingen specialreglering om tillsyn. Bestämmelserna om behandling av personuppgifter är enbart avsedda att komplettera eller ersätta personuppgiftslagen i något avseende, eftersom den reglerade verksamheten har ansetts behöva exempelvis en reglering som ytterligare stärker den registrerades integritetsskydd eller av andra skäl behöver en reglering utöver den som följer av personuppgiftslagen. Sägs här inget särskilt om tillsynsansvaret är det bara Datainspektionen som är tillsynsmyndighet.

I några av föreskrifterna förekommer däremot särregleringar om ansvaret för tillsyn. Vid sidan av Datainspektionen finns nämligen ett antal myndigheter med ett författningsreglerat uppdrag att utöva tillsyn över bland annat behandling av personuppgifter. I det följande beskrivs de föreskrifter som innehåller bestämmelser om behandling av personuppgifter och som dessutom har en reglering

som innebär att en annan myndighet än Datainspektionen har i uppdrag att utöva tillsyn över denna personuppgiftsbehandling.

En särskild fråga är hur ansvaret för tillsynen ska fördelas när en annan myndighet än Datainspektionen utövar tillsyn över en viss lag och denna, vilket normalt är fallet, endast innehåller några enstaka bestämmelser om personuppgiftsbehandling. För de frågor som inte är särreglerade i lagen gäller i sådana fall personuppgiftslagen när personuppgifter behandlas. Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen. Behandlingen av personuppgifter inom exempelvis ett register kan därmed ske med stöd av olika lagar och med olika behöriga tillsynsmyndigheter. Vi återkommer i kapitel 8 till frågan om och när en sådan fördelning av tillsynsansvar riskerar att skapa gränsdragningsproblem.

Som vår kartläggning visar ingår frågor om den granskade verksamhetens behandling av personuppgifter inte alltid i den tillsyn som faktiskt utförs av dessa myndigheter. Som framgår ovan har vi valt att tolka uppdraget så att regleringarna och myndigheterna ändå redovisas i detta sammanhang, så att bilden av dagens tillsyn över personuppgiftsbehandling ska bli så heltäckande som möjligt.

Behandling av personuppgifter i viss brottsbekämpande verksamhet

Säkerhets- och integritetsskyddsnämndens tillsyn över bland annat polisdatalagen

Polisdatalagen (2010:361) gäller vid behandling av personuppgifter i den brottsbekämpande verksamheten inom Polismyndigheten och Säkerhetspolisen, samt vid polisiärt arbete vid Ekobrottsmyndigheten. I lagen finns bland annat bestämmelser om för vilka ändamål personuppgifter får behandlas, bevarande, gallring och utlämnande av personuppgifter samt hur personuppgifter får göras gemensamt tillgängliga för den brottsbekämpande verksamheten. Enligt lagen (2010:362) om polisens allmänna spaningsregister får vidare uppgifter om brottsmisstänkta personer under vissa förutsättningar registreras i ett spaningsregister. Lagen anger bland annat vilka uppgifter som får behandlas och för vilka ändamål samt vad som gäller om sökning i registret, gallring och rättelse.

Säkerhets- och integritetsskyddsnämnden (SIN) utövar tillsyn över den behandling av personuppgifter enligt polisdatalagen och lagen om polisens allmänna spaningsregister som utförs i brottsbekämpande verksamhet av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten. När det gäller Säkerhetspolisen ska tillsynen även avse sådan personuppgiftsbehandling som följer av den förra polisdatalagen (1998:622). Utöver dessa uppgifter ska SIN också utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

SIN:s verksamhet regleras i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och i förordningen (2007:1141) med myndighetens instruktion. SIN:s tillsyn avser endast polisens personuppgiftsbehandling enligt de nämnda lagarna. Därmed omfattas inte personuppgiftsbehandling i enskild verksamhet av tillsynen. Dessutom omfattas bara myndigheternas personuppgiftsbehandling i brottsbekämpande verksamhet av SIN:s tillsyn. Personuppgiftsbehandling i exempelvis polisens personaladministrativa verksamhet regleras av personuppgiftslagen, och för denna tillsyn ansvarar Datainspektionen.

SIN är en relativt ny myndighet som började sin verksamhet 2008. Bakgrunden till inrättandet var, förutom behovet av ett fristående och självständigt organ för tillsyn över de brottsbekämpande myndigheternas ökade möjligheter att använda hemliga tvångsmedel, att Europadomstolen i en dom slagit fast att det i Sverige saknades ett tillgängligt effektivt rättsmedel för att få en uppgift avlägsnad från Säkerhetspolisens register. Domstolen konstaterade att tillsyn kan utövas av Justitiekanslern, Justitieombudsmannen, Datainspektionen och Registernämnden,[10] men fann att dessa rättsmedel inte ens sammantagna uppfyllde kravet på ett effektivt rättsmedel enligt artikel 13 i Europakonventionen.[11]

Den tillsyn som SIN bedriver ska särskilt avse sådan behandling som gäller s.k. känsliga personuppgifter, dvs. uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Tillsynen

[10] Registernämnden upphörde när SIN inrättades, och SIN övertog Registernämndens uppgifter.
[11] Europadomstolens dom 6 juni 2006 i målet Segerstedt-Wiberg m.fl. mot Sverige. Domen och dess betydelse för hur tillsynen bör vara utformad berörs ytterligare i avsnitt 10.3.2.

ska särskilt syfta till att säkerställa att personuppgiftsbehandlingen görs i enlighet med lag eller annan författning. När SIN beslutar att inleda ett initiativärende görs detta främst utifrån en bedömning av i vilken verksamhet hos de aktuella myndigheterna det finns en särskild risk för felaktig personuppgiftsbehandling. SIN utövar sin tillsyn genom inspektioner och andra undersökningar. Inspektionerna kan vara oanmälda, men hittills har alla inspektioner varit överenskomna i förväg. Myndigheten brukar dock inte i detalj i förväg redogöra för vad den avser att inspektera.

SIN ska också på begäran av en enskild person kontrollera om han eller hon har varit föremål för behandling av personuppgifter hos polisen och om behandlingen har skett i enlighet med lag eller annan författning. Alla personer, oavsett medborgarskap, har rätt att begära att en sådan kontroll genomförs. När kontrollen är genomförd ska den enskilde underrättas om detta. Sekretess kan hindra att den enskilde får närmare besked om resultatet av kontrollen, dvs. om polisen har behandlat uppgifter om den enskilde eller inte och vad de eventuella uppgifterna avsåg. Normalt omfattas uppgifter om huruvida den enskilde förekommer i Säkerhetspolisens register av sekretess. Om SIN vid sin kontroll upptäcker en felaktig personuppgiftsbehandling är SIN under vissa förutsättningar skyldig att anmäla detta till andra myndigheter. Den enskilde underrättas normalt om att en sådan anmälan har gjorts. På grund av sekretessen kan dock oftast ingen närmare information lämnas om varför uppgifterna har behandlats.

De myndigheter som omfattas av SIN:s tillsyn har en skyldighet att lämna de uppgifter och det biträde som SIN begär. Också domstolar och förvaltningsmyndigheter, som inte omfattas av tillsynen, är skyldiga att på begäran lämna upplysningar.

Ett tillsynsärende avslutas normalt med att SIN uttalar sig om sina iakttagelser och bedömningar och, om det behövs, om det enligt SIN finns ett behov av förändringar i den granskade verksamheten. SIN kan också uppmärksamma regeringen på eventuella behov av lagstiftningsåtgärder. Om SIN i sin verksamhet uppmärksammar felaktigheter som kan medföra ett skadeståndsansvar för staten ska SIN anmäla detta till Justitiekanslern. SIN ska också

anmäla vissa förhållanden till bland annat Åklagarmyndigheten eller Datainspektionen.[12]

När SIN inrättades betonades att dess verksamhet inte skulle överlappa utan komplettera den tillsyn som utförs av andra myndigheter, främst Datainspektionen, Justitiekanslern och Åklagarmyndigheten. SIN har heller inte sådana särskilda befogenheter som framför allt Datainspektionen har, såsom att i ett rättsligt bindande beslut föreskriva om rättelse eller förbud mot fortsatt behandling. Mot denna bakgrund infördes bestämmelserna om SIN:s samråd med och anmälningar till andra myndigheter.[13] SIN ska anmäla sina iakttagelser och överlämna relevanta delar av det som har framkommit i tillsyns- eller kontrollärendet till den myndighet som ansvarar för den aktuella frågan.

Nämndens uttalanden kan inte överklagas.

Antalet ärenden, både sådana som avser personuppgiftsbehandling inom polisen[14] och andra ärendekategorier, varierar påtagligt från år till år. Av det totala antalet ärenden som inleddes på SIN:s eget initiativ under 2014 (26 ärenden) avsåg 6 ärenden (23 %) personuppgiftsbehandling inom polisen. För 2013 avsåg 11 ärenden av totalt 19 (58 %) polisens personuppgiftsbehandling. 2012 inleddes totalt 65 ärenden på nämndens initiativ, varav 11 (17 %) avsåg polisens personuppgiftsbehandling. Övriga s.k. initiativärenden avser till största delen användningen av hemliga tvångsmedel och, med något enstaka ärende per år, användningen av kvalificerade skyddsidentiteter. Även om antalet ärenden om användningen av hemliga tvångsmedel är betydligt större än antalet ärenden om polisens personuppgiftsbehandling, ägnas enligt nämndens kansli ungefär lika mycket tid åt vartdera tillsynsområde.

Även antalet ärenden om enskildas begäran om kontroll av om de har varit föremål för personuppgiftsbehandling inom polisen varierar från år till år. 2014 inkom knappt 2 000 sådana ansökningar, 2013 drygt 400 och 2012 inkom 49 ansökningar.[15]

---

[12] 20 § i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

[13] Prop. 2006/07:133 s. 62.

[14] Statistikuppgiftuppgifterna avser tillsynsärenden om personuppgiftsbehandling inom både Säkerhetspolisen och den öppna polisen.

[15] Det stora antalet ansökningar 2014 förklaras av det uppmärksammade ärendet om det s.k. kringsresanderegistret vid den dåvarande Polismyndigheten i Skåne (SIN:s ärende med dnr 173-2013).

Antalet årsarbetskrafter som arbetar huvudsakligen med tillsyn över behandling av personuppgifter uppskattas av SIN till mellan 5 och 6.[16]

Behandling av personuppgifter i försvarsunderrättelseverksamhet

Försvarsunderrättelseverksamheten bedrivs till stöd för Sveriges utrikes-, säkerhets- och försvarspolitik och för att kartlägga yttre hot mot landet. Verksamheten regleras ibland annat lagen (2000:130) om försvarsunderrättelseverksamhet. Statens inspektion för försvarsunderrättelseverksamheten (Siun) har till uppgift att kontrollera att den försvarsunderrättelseverksamhet som bedrivs av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut sker i enlighet med lagar och andra föreskrifter. Siun ska även på enskilds begäran bland annat kontrollera om hans eller hennes meddelande har inhämtats i samband med signalspaning.

Siun granskar behandlingen av personuppgifter enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Siuns granskningsuppgift inskränker inte Datainspektionens övergripande tillsynsansvar utan utgör en särskild granskning i syfte att kompensera för enskildas begränsade möjligheter till insyn i personuppgiftsbehandlingen inom försvarsunderrättelseverksamheten.

Den tillsyn av behandling av personuppgifter som bedrivs vid Siun omfattas enligt direktiven inte av vårt uppdrag.[17]

[16] Antalet inkluderar administrativa uppgifter på tillsynsområdet.
[17] Dir. 2014:164 s. 6.

Behandling av personuppgifter inom elektronisk kommunikation

Post- och telestyrelsens tillsyn över bland annat lagen om elektronisk kommunikation

Lagen (2003:389) om elektronisk kommunikation (LEK), och den tillhörande förordningen (2003:396), gäller elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning. Lagen är inte tillämplig på det innehåll som överförs i elektroniska kommunikationsnät (1 kap. 4 § LEK).

I LEK finns bestämmelser om behandling av trafikuppgifter och om integritetsskydd. I den utsträckning LEK innehåller särskilda bestämmelser om behandling av personuppgifter som avviker från personuppgiftslagen, är LEK tillämplig och Post- och telestyrelsen (PTS) tillsynsmyndighet. PTS har ett samlat ansvar inom postområdet och området för elektronisk kommunikation. I detta ansvar ingår ett flertal tillsynsuppgifter. PTS har också uppgifter som nationell tillsynsmyndighet enligt EU-förordningar på området för elektronisk kommunikation. För annan behandling av personuppgifter inom området för elektronisk kommunikation gäller personuppgiftslagen, med Datainspektionen som tillsynsmyndighet.

PTS:s tillsynsansvar omfattar mer än behandlingen av personuppgifter och skyddet av den personliga integriteten vid sådan behandling. Fokus i LEK och för PTS är säker kommunikation, och detta gäller även om kommunikationen inte innehåller några personuppgifter. Till stor del avser tillsynsverksamheten vidare sådant som är kopplat till förutsättningarna för en effektiv konkurrens på marknaden för elektronisk kommunikation.

Tillsynen avser huvudsakligen personuppgiftsbehandling som utförs av enskilda eftersom operatörerna på marknaden för elektronisk kommunikation är privata företag. Tillsynen över den s.k. cookie-bestämmelser[18] omfattar dock även offentlig verksamhet.

Inom området för elektronisk kommunikation kan här också nämnas lagen (2006:24) om nationella toppdomäner för Sverige på

[18] Se mer om bestämmelsen och vad som menas med en cookie i kapitel 10.

internet och den s.k. eIDAS-förordningen.[19] PTS är tillsynsmyndighet även enligt dessa bestämmelser.

De befogenheter PTS har som tillsynsmyndighet motsvarar till stor del de som Datainspektionen har. Så har PTS bland annat rätt att få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av tillsynen, och kan meddela de förelägganden och förbud som behövs för att en felaktig personuppgiftsbehandling ska rättas. Följs inte förelägganden eller förbud kan PTS återkalla tillstånd, ändra tillståndsvillkor eller besluta att den som åsidosatt skyldigheten helt eller delvis ska upphöra med verksamheten (7 kap. 4 och 5 §§ LEK).

Utöver ett renodlat tillsynsansvar har PTS också i uppdrag att beskriva och analysera utvecklingen och resultatet inom området för elektronisk kommunikation och rapportera detta till regeringen (1 § förordningen [2007:952] med instruktion). Med detta avses även frågor om integritetsskydd vid behandlingen av personuppgifter. I myndighetens årsredovisningar redovisas bland annat sådana iakttagelser som rör integritetsfrågor. Myndigheten bedriver dessutom en omfattande och systematisk omvärldsbevakning inom olika verksamhetsområden, även integritetsområdet, som kan ligga till grund för bland annat den egna långsiktiga verksamhetsplaneringen.

PTS:s beslut enligt LEK, dvs. exempelvis ett beslut om förbud eller indraget tillstånd, kan överklagas till allmän förvaltningsdomstol.

Av myndighetens cirka 300 tillsynsärenden per år avser omkring 30 ärenden integritetsfrågor. Till detta kommer viss utredningsverksamhet som är relaterad till tillsyn men som inte avser enskilda tillsynsärenden. PTS uppskattar att sju årsarbetskrafter ägnar sig åt huvudsakligen tillsynsverksamhet. Härutöver tar myndigheten varje år emot cirka 300 frågor eller klagomål från allmänheten som rör integritetsfrågor, vilket motsvarar 5–10 procent av det totala antalet frågor och klagomål. Medias och allmänhetens intresse för frågor som rör telekommunikation rör dessutom förhållandevis ofta integritetsaspekter kring exempelvis trafikdatalagring och cookies.

[19] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Förordningen ersätter sedan den 1 juli 2016 lagen (2000:832) om kvalificerade elektroniska signaturer.

Behandling av personuppgifter vid kameraövervakning

Länsstyrelsernas och Datainspektionens tillsyn över kameraövervakningslagen

Övervakning med hjälp av kameror eller liknande utrustning kan få ske om intresset av sådan övervakning väger tyngre än den enskildas intresse av att inte bli övervakad. Kameraövervakning och behandling av ljud- och bildmaterialet från övervakningen innebär en behandling av personuppgifter, om informationen i materialet går att hänföra till en fysisk person som är i livet. Kameraövervakningslagens (2013:460) syfte är att tillgodose behovet av kameraövervakning för berättigade ändamål, samtidigt som enskilda skyddas mot otillbörligt intrång i den personliga integriteten. Det finns i lagen, utöver krav på tillstånd för viss kameraövervakning, bland annat bestämmelser om krav på att skydda materialet, begränsningar i hur länge bildupptagningar får bevaras samt skyldighet att informera om att en plats är övervakad. Dessutom finns bestämmelser som innebär begränsningar i vem som får ha tillgång till upptagningarna och för vilka ändamål de får användas.

Tillstånd krävs som huvudregel för övervakning av platser dit allmänheten har tillträde. Det är länsstyrelsen i respektive län som handlägger frågor om tillstånd och som tar emot anmälningar. Det är också länsstyrelserna som utövar den s.k. operativa tillsynen över kameraövervakning som sker på platser dit allmänheten har tillträde. Datainspektionen utövar tillsyn över kameraövervakning som bedrivs på platser dit allmänheten inte har tillträde (39 § respektive 40 § kameraövervakningslagen, och 2 § kameraövervakningsförordningen [2013:463]).

Både länsstyrelserna och Datainspektionen har rätt att inom ramen för sin tillsynsverksamhet meddela de förelägganden som behövs för att kameraövervakningslagen, och de föreskrifter och beslut som har meddelats med stöd av lagen, ska följas. Ett sådant föreläggande får förenas med vite.[20] De har rätt till tillträde till lokaler, till upplysningar samt till ljud- och bildmaterial.

Tillsynsmyndigheterna tar själva initiativ till ett tillsynsärende. Det finns därmed ingen skyldighet att pröva en anmälan exem-

[20] Se dock ovan vad som anses gälla om vitesföreläggande mot en annan statlig myndighet (avsnitt 6.2.2).

pelvis av någon som anser sig ha blivit felaktigt kameraövervakad eller på annat sätt utsatt för felaktig behandling av uppgifterna från sådan övervakning. Myndigheternas beslut får överklagas till allmän förvaltningsdomstol. Datainspektionen utövar dessutom sedan 2013 tillsyn över länsstyrelsernas tillståndsgivning med rätt att överklaga länsstyrelsernas beslut om kameraövervakning för att tillvarata allmänna intressen (47 § kameraövervakningslagen).

Datainspektionen har härutöver det centrala, övergripande ansvaret för tillsynen över kameraövervakningslagen. I detta ingår enligt 1 § kameraövervakningsförordningen att utvärdera rättstillämpningen, utvärdera, följa upp och samordna den operativa tillsynen, ge råd och stöd till länsstyrelserna, samt att ge information och råd till allmänheten och till dem som tillhandahåller och använder övervakningsutrustning. Enligt förarbetena bör det i det centrala tillsynsansvaret dessutom ingå att sammanställa praxis och att samla in fakta och erfarenheter om bland annat teknikutvecklingen och den internationella utvecklingen.[21]

Den kameraövervakning som omfattas av tillsynen kan utföras i både offentlig och privat verksamhet.

Datainspektionen har i egenskap av central tillsynsmyndighet på kameraövervakningsområdet initierat och upprätthållit en löpande samverkan med landets länsstyrelser. Inom ramen för denna samverkan hålls bland annat återkommande möten där praxis gås igenom och följs upp. Datainspektionen kan på detta sätt notera eventuella olikheter i tillämpningen av kameraövervakningslagen och verka för att sådana olikheter undviks. Härutöver arbetar Datainspektionen för att sprida kunskap om kameraövervakningslagen genom framtagande av informationsmaterial, anordnanden av konferenser, utveckling av myndighetens upplysningstjänst och genom att tillhandahålla teknisk kompetens på kameraövervaknings- och it-säkerhetsområdena. Möjligheten att överklaga länsstyrelsernas beslut används parallellt med uppgifterna som central tillsynsmyndighet för att så långt som möjligt bidra till att tillämpningen av kameraövervakningslagen ska bli korrekt och konsekvent.

Länsstyrelserna fattar årligen många hundra beslut i tillstånds- och tillsynsärenden. Datainspektionen granskar alla beslut för att överväga om det finns ett behov av att överklaga. Härutöver avgör

[21] Prop. 2012/13:115 s. 129 f.

Datainspektionen en handfull ärenden per år inom ramen för det centrala tillsynsansvaret respektive ansvaret för tillsynen över kameraövervakning på platser dit allmänheten inte har tillträde.

Kameraövervakningslagen är för närvarande föremål för utredning i Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14, dir. 2015:125). Utredningen har i juni 2016 genom tilläggsdirektiv fått ett utvidgat uppdrag som omfattar att även anpassa regleringen i lagen till den nya EU-rättsliga dataskyddsregleringen (dir. 2016:54). I detta ingår att analysera hur den nya EU-regleringen påverkar utrymmet att i nationell rätt reglera den personuppgiftsbehandling som kameraövervakning innebär. Av tilläggsdirektiven framgår vidare att en fråga som utredaren behöver analysera särskilt är hur den nya EU-rättsliga dataskyddsregleringens bestämmelser om tillsynsmyndigheter förhåller sig till organisationen av tillsynen över kameraövervakning i Sverige. Utredningen ska lämna de författningsförslag som behövs och är lämpliga och ska vid genomförandet av uppdraget ta hänsyn till de förslag som vår utredning lämnar. Utredningen ska redovisa sitt uppdrag den 15 juni 2017.

Eftersom frågan om den framtida regleringen av den personuppgiftsbehandling som kameraövervakning innebär, liksom hur tillsynen häröver bör vara utformad och organiserad, är under utredning, avstår vi från att göra några närmare överväganden i fråga om tillsyn över behandling av personuppgifter vid kameraövervakning.

Personuppgiftsbehandling inom vård och omsorg

Inspektionens för vård och omsorg tillsyn över bland annat patientdatalagen

Bestämmelserna om behandling av personuppgifter inom vård och omsorg finns huvudsakligen i patientdatalagen (2008:355) och i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten. Lagarna reglerar bland annat begränsningar av vem som ska ha åtkomst till patientuppgifter, vårdgivarens skyldighet att genomföra systematisk logguppföljning, vilka personuppgifter som får behandlas och när behandling får ske, förutsättningarna för s.k.

sammanhållen journalföring och patientens rätt att spärra uppgifter i journalsystem

Inspektionen för vård och omsorg (IVO) bildades 2013 och ansvarar för tillsynen över hälso- och sjukvården, socialtjänsten samt verksamhet enligt lagen (1993:387) om stöd och service till vissa funktionshindrade (LSS). Syftet med myndighetens tillsyn är att granska att befolkningen får vård och omsorg som är säker, har god kvalitet och bedrivs i enlighet med lagar och andra föreskrifter (2 § förordningen [2013:176] med instruktion för Inspektionen för vård och omsorg).

IVO:s tillsyn enligt patientdatalagen är huvudsakligen inriktad på patientsäkerhetsfrågor. En sådan tillsyn kan även innefatta frågor om behandling av personuppgifter. Det finns också bestämmelser om behandling av personuppgifter i andra föreskrifter, med IVO som angiven tillsynsmyndighet. Som exempel kan nämnas lagen (2006:496) om blodsäkerhet och lagen (2006:1570) om skydd mot internationella hot mot människors hälsa. Dessutom finns bestämmelser om behandling av personuppgifter i lagen (2003:460) om etikprövning av forskning som avser människor, där IVO har ett tillsynsansvar.

Även Datainspektionens tillsynsansvar omfattar patientdatalagen och frågor om behandling av personuppgifter inom vård och omsorg. Gränsdragningen mellan de båda myndigheternas ansvarsområden är inte alltid tydlig. Vi återkommer till detta förhållande i kapitel 8 och 10.

Verksamhet för vård och omsorg kan bedrivas både av offentliga och privata aktörer och de båda tillsynsmyndigheternas tillsyn omfattar båda dessa kategorier.

IVO uppger att det är svårt att ange eller ens uppskatta hur många tillsynsärenden per år som avser personuppgiftsbehandling eftersom de inte för någon sådan statistik. När det gäller ärenden om informationssäkerhet, som till viss del kan avse frågor om behandling av personuppgifter, fattade IVO under 2015 beslut i totalt 77 tillsynsärenden, grundade på både klagomål och s.k. lex Maria-anmälningar. Detta kan jämföras med det totala antalet beslut i klagomåls- och anmälningsärenden, som under samma år långt översteg 10 000.

Etikprövning inom forskning som innefattar personuppgiftsbehandling

Centrala etikprövningsnämndens tillsyn över etikprövningslagen

I syfte att skydda den enskilda människan och respekten för människovärdet i forskningen finns bestämmelser om etikprövning i lagen (2003:460) om etikprövning av forskning som avser människor (etikprövningslagen). Lagen ska tillämpas bland annat på forskning som innefattar en behandling av känsliga personuppgifter och av personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel m.m. Sådan forskning får bedrivas endast om den har godkänts vid en etikprövning. Etikprövningen ska bland annat beakta å ena sidan respekten för människovärdet, mänskliga rättigheter, om det förväntade resultatet kan uppnås med forskning som innebär mindre risker för forskningspersonernas hälsa, säkerhet och personliga integritet respektive å andra sidan intresset av forskningen.

Behandling av känsliga personuppgifter och personuppgifter om lagöverträdelser får godkännas bara om den är nödvändig för att forskningen ska kunna utföras. Till kravet på godkännande vid en etikprövning kommer som huvudregel ett krav på samtycke av den person som forskningen avser. Behandlingen av personuppgifter inom ramen för forskningen måste sedan följa reglerna i personuppgiftslagen.

Etikprövningen utförs av regionala etikprövningsnämnder. Det finns dessutom en central nämnd, Centrala etikprövningsnämnden, som ska pröva ärenden som har överlämnats dit av en regional nämnd eller beslut meddelade av de regionala nämnderna som har överklagats. Centrala etikprövningsnämnden utövar också tillsyn över att etikprövningslagen följs, vilket inkluderar behandlingen av personuppgifter inom sådan forskning som omfattas av lagen. Tillsynsansvaret är dock negativt formulerat, så att nämnden ska utöva tillsyn endast i den mån tillsynen inte faller inom en annan myndighets tillsynsområde. I förarbetena anges att sådana myndigheter är Socialstyrelsen (vars uppgifter i detta avseende sedan dess har övertagits av IVO), Läkemedelsverket och Datainspek-

tionen.[22] Viss oklarhet råder om ansvarsfördelningen mellan Centrala etikprövningsnämnden och Datainspektionen, vilket vi berör ytterligare i kapitel 8 och 10. Det har förekommit att ärenden har överlämnats av Centrala etikprövningsnämnden till Datainspektionen, som emellertid inte heller har ansett sig vara rätt myndighet att utöva tillsyn. Resultatet av denna oenighet är att inte någon myndighet har utövat tillsyn över dessa ärenden.

Centrala etikprövningsnämnden uppskattar att knappt hälften av de tillsynsärenden som kommer in till nämnden rör behandling av personuppgifter, vilket inte motsvarar mer än en handfull ärenden per år. Nämndens uppfattning är emellertid i de allra flesta av dessa fall att den inte är behörig att utöva tillsyn. Om behandlingen gäller s.k. känsliga personuppgifter överlämnas ärendet alltid till Datainspektionen. Centrala etikprövningsnämndens arbete med tillsyn över behandling av personuppgifter är därmed mycket begränsad och uppskattas av nämndens kansli motsvara tio procent av en årsarbetskraft.

En särskild utredare har fått i uppdrag att se över etikprövningslagen (U 2016:02, dir. 2016:45). I uppdraget ingår bland annat att bedöma om regleringen av tillsynen över lagen och föreskrifter som meddelats med stöd av lagen behöver ändras. I direktiven till utredningen konstateras emellertid att frågor om tillsyn över behandling av personuppgifter omfattas av vår utredning.

Behandling av personuppgifter vid s.k. spam

Konsumentverkets tillsyn över spambestämmelsen i marknadsföringslagen

Av 19 § marknadsföringslagen (2008:486) följer ett förbud mot s.k. obeställd reklam till fysiska personer via exempelvis e-post. Förbudet innebär att reklamutskick får skickas till en fysisk person endast om denne har samtyckt till det på förhand eller i vart fall, i samband med ett tidigare köp, inte har motsatt sig att e-postadressen används för marknadsföring. Sådana utskick av marknadsföring, som ofta kallas spam, innebär en behandling av personuppgifter.

[22] Prop. 2002/03:50 s. 163 f.

Förbudet mot obeställd reklam, liksom marknadsföringslagen i övrigt, gäller näringsidkare som marknadsför sina produkter. Tillsynen i denna del riktar sig därmed mot privata aktörer.

Konsumentverket utövar tillsyn över att marknadsföringslagen, inklusive bestämmelsen om förbudet mot obeställd reklam, följs. Av i genomsnitt cirka 600 tillsynsärenden per år avser en handfull[23] ärenden per år spam via e-post. Ytterligare ett fåtal avser spam via sms. Tillsynsärendena grundar sig på anmälningar från privatpersoner, och avser ofta bolag som har varit föremål för många anmälningar. Under 2015 gjordes drygt 2 500 anmälningar (av 850 personer) om spam via e-post. Ett av de tillsynsärenden som inleddes under året avsåg ett bolag som hade varit föremål för närmare 100 anmälningar.

Behandling av personuppgifter vid åtgärder mot penningtvätt och finansiering av terrorism

Penningtvättslagen – ett delat tillsynsansvar

Lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) syftar till att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt och finansiering av terrorism. Lagen gäller för fysiska och juridiska personer som driver rörelser som avser bland annat bank- och finansiering, fastighetsmäklarverksamhet, bokföring eller revision, advokatverksamhet och yrkesmässig handel med varor mot kontant betalning. Lagen, och det penningtvättsdirektiv som lagen bygger på, ställer krav på att verksamhetsutövare ska vidta åtgärder för att kontrollera sina kunder. Misstänkta transaktioner ska anmälas till Finanspolisen.

Den 20 maj 2015 antog Europaparlamentet och rådet det fjärde penningtvättsdirektivet. Bestämmelserna i det nya direktivet ska vara införlivade i nationell rätt senast den 26 juni 2017.

Kontrollerna enligt penningtvättslagen innebär normalt en automatiserad behandling av personuppgifter. I lagen finns vissa bestämmelser om verksamhetsutövares behandling av personuppgifter, som till viss del ersätter personuppgiftslagen.

[23] 2015 inleddes tre ärenden, 2014 tio ärenden och 2013 ett ärende.

Det finns också bestämmelser om tillsyn för viss verksamhet som omfattas av lagen. För tillsyn av annan verksamhet hänvisas till bestämmelser i andra lagar. Genom tillsynen ska kontrolleras att verksamheten bedrivs i enlighet med penningtvättslagen och föreskrifter som har meddelats med stöd av lagen (6 kap. 2 §). Förarbetena anger att tillsynen bland annat ska innebära en kontroll av att de som står under tillsyn har rutiner för att kontrollera identiteten hos personer som vill inleda en sådan affärsförbindelse som omfattas av lagen.[24]

Länsstyrelserna i Stockholms, Västra Götalands och Skåne län ska utöva tillsyn över viss verksamhet som omfattas av penningtvättslagen (16 § förordningen [2009:92] om åtgärder mot penningtvätt och finansiering av terrorism). Den verksamhet som omfattas av länsstyrelsernas tillsyn är den som utförs av redovisningskonsulter, skatterådgivare, vissa oberoende jurister, bolagsmäklare, och verksamhetsutövare som säljer varor mot kontant betalning överstigande 15 000 euro. (1 kap. 2 § 11, 12 och 14–16 penningtvättslagen).

Härutöver utövas tillsyn över verksamheter som omfattas av penningtvättslagen av olika tillsynsorgan.

– Fastighetsmäklare granskas av Fastighetsmäklarinspektionen.
– Spelmarknaden står under tillsyn av Lotteriinspektionen. Ett kasinoföretag, Casino Cosmopol, är den enda aktör som för närvarande omfattas av penningtvättslagen och inspektionens tillsyn i de delarna.
– Revisorer och revisionsbolag granskas av Revisorsnämnden.
– Advokater och biträdande jurister vid advokatbyråer kontrolleras av Sveriges advokatsamfund.
– Finansinspektionen utövar tillsyn över finansiella aktörer såsom banker och finansieringsrörelser, fondverksamhet m.m. Härutöver har Finansinspektionen i uppdrag att samordna tillsynen enligt penningtvättslagen. Vid myndigheten finns ett samordningsorgan, där övriga tillsynsmyndigheter och Sveriges advokatsamfund finns representerade.

[24] Prop. 2008/09:70 s. 160.

Behandling av personuppgifter i kasinoverksamhet

Lotteriinspektionens tillsyn över kasinolagen

Av kasinolagen (1999:355) följer bland annat att den som anordnar kasinospel ska föra ett register över kasinots besökare. Registret får föras med hjälp av automatiserad behandling och ska innehålla uppgifter om besökarnas namn, personnummer och adress, samt ett fotografi av besökaren och uppgift om tidpunkten för besöket.

Casino Cosmopol, som är den enda aktör på den svenska spelmarknaden som för närvarande omfattas av kasinolagen, registrerar uppgifterna i ett särskilt besöksregister som kallas CMS. Registret motsvarar också den nämnda penningtvättslagens krav på kundkännedom. CMS-registret innebär att personuppgifter behandlas och att behandlingen kan vara automatiserad. Härutöver kan gästerna i ett kasino kameraövervakas, vilket i sig innebär att personuppgifter behandlas. Slutligen registreras vissa kunduppgifter i kasinots s.k. händelserapporteringssystem iTrak. Uppgifterna används exempelvis för att registrera personer som är avstängda från spel på grund av spelöverträdelser och för att hantera ekonomiska förhållanden mellan ett kasino och dess besökare.

Lotteriinspektionen ansvarar för tillsynen över att lagen (1982:636) om anordnande av visst automatspel, lotterilagen och kasinolagen följs. Tillsyn av den personuppgiftsbehandling som sker med stöd av kasinolagen har genomförts av Lotteriinspektionen. Händelserapporteringssystemet iTrak omfattas inte av kasinolagen och därmed inte av Lotteriinspektionens tillsyn. När det gäller detta register är därför Datainspektionen den ansvariga tillsynsmyndigheten. Länsstyrelsen ansvarar för tillsynen över att kameraövervakningen bedrivs lagenligt (se ovan).

Tillsynen avser för närvarande bara verksamhet som bedrivs av privata aktörer. Tillsyn över den behandling av personuppgifter som följer av kasinolagen utgör enligt Lotteriinspektionen en begränsad del av inspektionens tillsynsverksamhet.

6.2.4 Vissa ytterligare tillsynsmyndigheter

Härutöver finns ytterligare en kategori författningar och tillsynsmyndigheter som vi anser bör redovisas i detta sammanhang. I den placerar vi föreskrifter som liksom de som nämnts i tidigare avsnitt innehåller bestämmelser om både personuppgiftsbehandling och tillsyn, men där vi bedömer att personuppgiftsbehandlingen är av begränsad omfattning och där vi utgår ifrån att den tillsyn som bedrivs av en utpekad tillsynsmyndighet i praktiken inte omfattar dessa frågor. Tillsynsansvaret kan i flertalet av dessa fall snarare betecknas som teoretiskt – regleringen om tillsyn är formulerat på ett sådant sätt att det omfattar även behandling av personuppgifter, men avsikten har sannolikt inte varit att sådana frågor faktiskt ska omfattas av myndighetens tillsyn. Vi återkommer i kapitel 10 till frågan om behovet av översyn av sådana bestämmelser.

Här finns också föreskrifter som innebär att en myndighet pekas ut som tillsynsmyndighet med uppdrag att utöva tillsyn över efterlevnaden av en lag som innehåller en eller flera uttryckliga bestämmelser om personuppgiftsbehandling, men där samma myndighet dessutom anges som personuppgiftsansvarig för samma behandling. Eftersom en och samma myndighet inte bör både vara personuppgiftsansvarig och utöva tillsyn över personuppgiftsbehandlingen, torde tillsynsuppgifterna i de aktuella fallen trots föreskrifternas formulering i själva verket inte omfatta personuppgiftsbehandlingen.

Som exempel på dessa typer av regleringar kan följande föreskrifter nämnas.

I lagen (2004:1199) om handel med utsläppsrätter regleras förutsättningar för handel med rätt att släppa ut växthusgaser. Statens energimyndighet ska föra ett register över svenska utsläppsrätter. Lagen innehåller vissa bestämmelser om behandlingen av personuppgifter i ett sådant register, i övrigt hänvisas till personuppgiftslagen. Av den tillhörande förordningen (2004:1205) följer att *Naturvårdsverket* är den tillsynsmyndighet som ska utöva tillsyn över att lagen följs.[25]

[25] Naturvårdsverket har uppgett att frågor om personuppgiftsbehandling inte har varit del av myndighetens tillsyn och att man inte hade uppfattat att lagen ger dem ett sådant tillsynsuppdrag.

Försäkringsförmedlare (dvs. juridiska eller fysiska personer som yrkesmässigt för någon annans räkning bland annat förmedlar och ingår försäkringsavtal) torde i sin verksamhet behandla personuppgifter. Förmedlarna står enligt lagen (2005:405) om försäkringsförmedling under tillsyn av *Finansinspektionen*. Tillsynen ska avse att den som utövar försäkringsförmedling följer försäkringsförmedlingslagen, föreskrifter som har meddelats med stöd av den lagen och andra författningar som reglerar försäkringsförmedlarens verksamhet. Förordningen (2005:411) om försäkringsförmedling innehåller bestämmelser om behandling av personuppgifter.

Lagen (2010:751) om betaltjänster reglerar tillhandahållandet av betaltjänster, dvs. tjänster som gör det möjligt att t.ex. genomföra betalningstransaktioner via autogiro och kontokort. Lagen innehåller bestämmelser om sådan behandling av personuppgifter som en betaltjänstleverantör kan genomföra som ett led i granskningen av transaktioner i syfte att avslöja bedrägerier. Av lagen följer också att *Finansinspektionen* ska utöva tillsyn över att bestämmelserna i lagen följs.[26]

I lagen (2011:725) om behörighet för lokförare finns bland annat bestämmelser om register över förarbevis m.m. för lokförare och om behandlingen av personuppgifter i sådana register. *Transportstyrelsen* utövar enligt förordningen (2011:728) om behörighet för lokförare tillsyn över att lagen följs. Samtidigt anges i lagen att det är tillsynsmyndigheten som för och är personuppgiftsansvarig för de s.k. förarbevisregistren. Ett av registren, ett s.k. intygsregister, med uppgifter om kompletterande intyg ska dock föras av järnvägsföretag och infrastrukturförvaltare, som då är personuppgiftsansvariga för registret. Regleringen innebär att Transportstyrelsens tillsynsansvar kan sägas omfatta intygsregistret, medan Datainspektionen ansvarar för tillsyn över de register som Transportstyrelsen är personuppgiftsansvarigt för.

Lagen (2011:1200) om elcertifikat innehåller bestämmelser om bland annat tilldelning av och handel med s.k. elcertifikat, som utfärdas för produktion av förnybar el. Ett elektroniskt register ska föras av den s.k. kontoföringsmyndigheten över tilldelade elcertifikat, och lagen innehåller vissa bestämmelser om behandlingen av

[26] Finansinspektionen har uppgett att frågor om personuppgiftsbehandling inte har varit föremål för inspektionens tillsyn enligt de nämnda lagarna.

personuppgifter i sådana register. Av förordningen (2011:1480) om elcertifikat följer att *Statens energimyndighet* är både kontoförings-myndighet och tillsynsmyndighet.

I skogsvårdslagen (1979:429) regleras bland annat anläggning, skötsel och avverkning av skog. Lagen innehåller bestämmelser om det automatiserade register som ska föras över fysiska och juridiska personer som yrkesmässigt bedriver produktion av och handel med skogsodlingsmaterial, och behandling av personuppgifter i ett sådant register. I lagen anges att *Skogsstyrelsen* ska utöva tillsyn över efterlevnaden av lagen. Samma myndighet är dock även personuppgiftsansvarig för registret.

Här finns slutligen exempel på tillsynsmyndigheter som ska granska att en verksamhet bedrivs lagenligt i största allmänhet, vilket åtminstone teoretiskt kan sägas omfatta även personuppgiftsbehandlingen i den granskade verksamheten. Som ett exempel kan nämnas att *Myndigheten för familjerätt och föräldraskapsstöd* ska utöva tillsyn över att de auktoriserade adoptionssammanslutningarnas arbete sker i enlighet med lag. *Kronofogdemyndigheten* är tillsynsmyndighet enligt konkurslagen (1987:672) och ska på motsvarande sätt övervaka att konkursförvaltningar bedrivs lagenligt.

6.2.5 Extraordinär tillsyn

Justitieombudsmannens och Justitiekanslerns tillsyn över den offentliga förvaltningen

Vid sidan av de ordinära tillsynsmyndigheterna utövas tillsyn över hur lagar och andra föreskrifter tillämpas i offentlig verksamhet av Riksdagens ombudsmän (Justitieombudsmannen, JO) och Justitiekanslern (JK). Denna tillsyn inbegriper givetvis behandlingen av personuppgifter och skyddet av enskildas personliga integritet vid sådan behandling. Som nämnts i kapitel 4 utgör både Justitieombudsmannens och Justitiekanslerns tillsynsverksamhet s.k. extraordinär tillsyn. Detta innebär bland annat att de inte kan ompröva beslut som har fattats av andra myndigheter och inte ändra dessa beslut. Ett tillsynsärende kan resultera i ett beslut som kan innehålla kritik, vägledande uttalanden och liknande men inte i rättsligt bindande beslut om exempelvis rättelse. Besluten är allmänt tillgängliga på respektive myndighet. De beslut som anses

vara av särskilt intresse, t.ex. på grund av sin vägledande funktion, publiceras dessutom på de båda myndigheternas webbplatser.

Justitieombudsmannens verksamhet regleras i regeringsformen, riksdagsordningen och lagen (1986:765) med instruktion för riksdagens ombudsmän. Justitiekanslerns verksamhet regleras, utöver i tryckfrihetsförordningen och yttrandefrihetsgrundlagen, främst i lagen (1975:1339) om Justitiekanslerns tillsyn, förordningen (1975:1345) med instruktion för Justitiekanslern och förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten.

De som står under de två tillsynsmyndigheternas tillsyn ska på begäran lämna upplysningar och yttranden, samt ge tillgång till handlingar och protokoll. Ett granskningsärende kan inledas både efter ett klagomål av en enskild och på myndighetens eget initiativ. Både Justitieombudsmannen och Justitiekanslern kan genomföra inspektioner som ett led i granskningen. Om en befattningshavare har begått sådana fel att det kan utgöra en brottslig handling, får en justitieombudsman eller justitiekanslern som särskild åklagare väcka åtal mot befattningshavaren. Befattningshavaren kan dessutom anmälas för disciplinpåföljd eller avskedande. Gäller misstankarna ett tryck- eller yttrandefrihetsbrott är det bara justitiekanslern som kan väcka sådant åtal.

Justitiekanslern hade tidigare möjlighet att för att ta tillvara allmänna intressen överklaga länsstyrelsernas beslut om kameraövervakning på platser dit allmänheten har tillträde. Sedan den nya kameraövervakningslagen trädde i kraft 2013 har denna uppgift övertagits av Datainspektionen (47 §). Justitiekanslern kan dock fortfarande överklaga beslut enligt den tidigare lagen (1998:150) om allmän kameraövervakning.

Som nämnts ska SIN anmäla till Justitiekanslern om nämnden i sin tillsyn har konstaterat brister i behandlingen av personuppgifter som kan medföra skadeståndsansvar för staten. Även i andra fall kan statens skadeståndsansvar för felaktig personuppgiftsbehandling aktualiseras, och det är även då Justitiekanslern som handlägger ärendena och som företräder staten (48 § personuppgiftslagen och 3 § förordningen [1995:1301] om handläggning av skadeståndsanspråk mot staten).

Myndigheters behandling av personuppgifter kan därmed bli föremål för tillsyn både av ett ordinarie tillsynsorgan, i de flesta fall Datainspektionen, och av de extraordinära. Medan Datainspek-

tionens tillsyn riktar sig enbart mot en myndighet som sådan i egenskap av personuppgiftsansvarig, kan Justitieombudsmannens och Justitiekanslerns tillsyn dessutom avse enskilda tjänstemän. Ett uttalande av de två senare tillsynsorganen kan därmed gälla både i vilken utsträckning en myndighet har fullgjort sin uppgift som personuppgiftsansvarig och om en enskild tjänsteman har behandlat personuppgifter på ett korrekt sätt.

7 Tillsynen över personuppgiftsbehandlingen i några andra länder

7.1 Inledning

I detta avsnitt beskrivs översiktligt hur den statliga tillsynen över behandlingen av personuppgifter är organiserad i Norge, Danmark och Finland. En sammanfattande beskrivning av hur tillsynen ser ut i övriga Europa och världen lämnas också. Beskrivningarna tar sikte på i vilken utsträckning ansvaret för tillsynen i andra länder är koncentrerat till en tillsynsmyndighet eller delat mellan flera.

7.2 Norge

Den centrala myndigheten för tillsyn över personuppgiftsbehandling i Norge är Datatilsynet. Det är en myndighet under regeringen som har uppgifter som till stor del motsvarar den svenska Datainspektionens. Tillsynen genomförs både genom tillsyn på eget initiativ och genom prövning av klagomål från allmänheten. Datatilsynet har ingen skyldighet att pröva klagomål, utan avgör självständigt vilka granskningsärenden de vill inleda med anledning av ett klagomål. Tillsynsinsatserna planeras ofta så att de exempelvis under en period koncentreras på en viss verksamhet som bedöms innebära särskilda integritetsrisker eller på sådana verksamheter som kan anses vara representativa för en större verksamhetssektor. Inspektioner kan genomföras både på plats och genom skriftlig kommunikation med den granskade verksamheten.

Datatilsynet jobbar aktivt för att skapa uppmärksamhet och öka medvetenheten kring integritetsfrågor, både hos allmänheten, lag-

stiftaren och bland dem som bedriver verksamhet som riskerar att påverka den personliga integriteten. Detta sker exempelvis genom informations- och rådgivningsverksamhet och genom att myndigheten deltar bland annat i den allmänna debatten och hålla föredrag vid konferenser och andra sammankomster. Myndigheten genomför också enkätundersökningar, kartläggningar om norrmännens inställning och förväntningar när det gäller integritetsfrågor och skyddet för den personliga integriteten.

Härutöver utövar det s.k. EOS-utvalget[1] tillsyn av underrättelse- och övervakningsverksamhet som avser rikets säkerhet vid de s.k. EOS-myndigheterna, dvs. främst säkerhetspolisen, den nationella säkerhetsmyndigheten och säkerhetsavdelningen inom försvaret. Den verksamhet som omfattas av tillsynen innebär ofta en behandling av personuppgifter. Utvalgets sju ledamöter väljs av stortinget för fem år, med möjlighet till omval, men utgör en fristående enhet i förhållande till Stortinget. Stortingsledamöter kan inte samtidigt vara ledamöter av utvalget.

EOS-utvalgets tillsyn avser skyddet för den enskildes rättigheter i den granskade verksamheten, såsom exempelvis att underrättelse- och övervakningsåtgärderna är proportionerliga i förhållande till det behov som föranleder dem och att den övervakades integritet inte kränks i högre grad än vad som anses nödvändigt. Enskilda som anser eller misstänker att de varit föremål för felaktig personuppgiftsbehandling eller andra åtgärder kan anmäla detta till utvalget, som är skyldigt att utreda alla anmälningar. Om utvalget finner att det har förekommit felaktigheter i det granskade ärendet konstateras detta i ett skriftligt yttrande till den berörda myndigheten, som ombeds att rätta till felaktigheterna och i förekommande fall kompensera anmälaren för eventuella skador. Utvalget kan inte meddela bindande beslut om rättelser, skadestånd eller andra åtgärder.

Vidare utövas i Norge tillsyn av motsvarigheten till den svenska Post- och telestyrelsen: Nasjonal kommunikasjonsmyndighet (Nkom), bland annat över behandlingen av personuppgifter i post- och telekommunikation.

[1] Stortingets kontrollutvalg for etterrettnings-, overvåknings- og sikkerhetstjeneste.

7.3 Danmark

Den centrala tillsynsmyndigheten på dataskyddsområdet heter även i Danmark Datatilsynet. Myndighetens huvudsakliga uppgift är att verka för att den danska personuppgiftslagen följs. Detta sker huvudsakligen genom förebyggande arbete såsom rådgivning och informationskampanjer, men också genom tillsyn. Tillsynsärenden kan inledas både efter anmälningar och på myndighetens eget initiativ. En person som anser sig ha blivit utsatt för felaktig personuppgiftsbehandling ska i första hand vända sig till den personuppgiftsansvarige och kräva rättelse. Om detta inte sker kan en anmälan göras till Datatilsynet, som då är skyldig att inleda ett tillsynsärende.

Datatilsynet ska dessutom alltid få yttra sig över förslag till lagar och andra föreskrifter som rör skyddet för den personliga integriteten.

Datatilsynet består av ett sekretariat och ett beslutande råd, Datarådet, vars ledamöter utses av justitieministern. Rådets ordförande ska vara domare. I övrigt består rådet för närvarande bland annat av en advokat, en professor i juridik och en direktör för en konsumentorganisation. Rådet beslutar i ärenden av principiell karaktär och i ärenden som har ett stort allmänt intresse. Sekretariatet ansvarar för myndighetens löpande arbete.

Ett tillsynsärende kan resultera i ett yttrande av Datatilsynet, som också kan kräva rättelse och förbjuda ytterligare personuppgiftsbehandling. Datatilsynets beslut kan inte överklagas.

Härutöver utövas i Danmark tillsyn över personuppgiftsbehandling av ytterligare några myndigheter. Domstolsstyrelsen utövar tillsyn över domstolarnas behandling av personuppgifter i den administrativa verksamheten. Tilsynet med Efterretningstjenesterne (TET) utövar tillsyn över personuppgiftsbehandlingen i polisens och försvarsmaktens underrättelseverksamhet samt i Center for Cybersikkerhed. På begäran av enskilda ska vidare TET kontrollera om den enskilde har varit föremål för personuppgiftsbehandling inom underrättelseverksamheterna.

Tillsyn över att bestämmelserna om s.k. cookies (dvs. en textfil som en webbplats begär att få spara i en besökares dator för att följa hur besökaren använder webbplatsen) och över övriga bestäm-

melser som följer av det s.k. e-privacy-direktivet[2] utövas i Danmark av Erhversstyrelsen.[3]

Den danska konsumentombudsmannen utövar tillsyn över förbudet mot s.k. spam (obeställd reklam via bland annat e-post).

7.4 Finland

I Finland är tillsynen över behandling av personuppgifter i huvudsak koncentrerad till de två s.k. datasekretessmyndigheterna Dataombudsmannen och Datasekretessnämnden.

Dataombudsmannens uppgifter motsvarar i stor utsträckning den svenska Datainspektionens. Myndigheten ska främja god informationshantering och ska genom anvisningar och rådgivning verka för att den finska personuppgiftslagen följs och kränkningar av den personliga integriteten undviks. Personuppgiftsbehandling ska anmälas till ombudsmannen och enskilda som har registrerats kan genom klagomål kräva prövning av om en personuppgiftsbehandling är laglig. Dataombudsmannen är skyldig att pröva sådana klagomål. Ombudsmannens kan efter genomförd tillsyn emellertid endast ge råd och anvisningar om den fortsatta personuppgiftsbehandlingen; besluten är, annat än i undantagsfall, inte bindande.

En stor del av Dataombudsmannens arbete ägnas åt förebyggande arbete, med information om lagstiftningen som rör behandlingen av personuppgifter och skyddet av den personliga integriteten. Vid all ny lagstiftning som rör den personliga integriteten ska Dataombudsmannen vidare medverka under beredningen och vid behov skriva ett utlåtande. Innan en åklagare väcker åtal för personuppgiftsbrott ska ombudsmannen höras, och domstolen ska bereda ombudsmanen tillfälle att yttra sig innan sådana mål avgörs. Dataombudsmannen medverkar dessutom vid utarbetandet av s.k. uppförandekodexar i olika branscher och har tagit fram ett ”gör-det-själv-test” som innebär att registeransvariga på egen hand kan kontrollera om deras behandling av personuppgifter är lagenlig.

[2] Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.
[3] Erhversstyrelsen motsvaras i Sverige av Bolagsverket. Tillsyn över bland annat sådan behandling av personuppgifter som regleras i e-privacydirektivet utövas i Sverige dock av Post- och telestyrelsen.

Dataombudsmannen genomför inspektioner, både på plats i den registeransvariges lokaler och genom skriftväxling, och har rätt att få tillgång till de registrerade uppgifterna och till all annan information som behövs för att utöva tillsynen. Ibland anlitas särskilda sakkunniga för genomförande av tillsynsverksamheten.

Dataombudsmannen kan hänskjuta ärenden som bedöms vara principiellt viktiga till Datasekretessnämnden. Nämnden har i dessa ärenden samma rätt att få information och uppgifter som Dataombudsmannen. Nämnden består av en ordförande, en vice ordförande och fem ytterligare ledamöter som förordnas av regeringen för tre år i taget. Alla ledamöter ska ha erfarenhet av registerverksamhet. Härutöver ska ordföranden, vice ordföranden och minst en ledamot vara jurister. Den egentliga beslutanderätten i ärenden om felaktig personuppgiftsbehandling ligger i nämnden. Ombudsmannen kan dock själv fatta beslut om rätt för den registrerade att få insyn i de behandlade uppgifterna och om rättelse.

Datasekretessnämnden har också till uppgift att utfärda föreskrifter om behandlingen av personuppgifter och att följa utvecklingen på området för behandling av personuppgifter och integritetsskydd, och att bedöma behovet av exempelvis lagstiftningsåtgärder. Den senare uppgiften har även Dataombudsmannen.

Datasekretessnämnden kan förbjuda fortsatt behandling av personuppgifter som anses strida mot personuppgiftslagen eller andra föreskrifter, besluta om rättelse och om återkallelse av tillstånd.

Utöver den tillsyn som utförs av Dataombudsmannen och Datasekretessnämnden utövar myndigheten Kommunikationsverket tillsyn över den personuppgiftsbehandling som omfattas av e-privacydirektivet. Detta omfattar också bestämmelser om tillåtligheten av s.k. cookies.

Det finns i Finland inga särskilda tillsynsmyndigheter med ansvar för personuppgiftsbehandling inom polisens eller försvars- och underrättelsemyndigheternas verksamhet.

7.5 Några andra länder i Europa och övriga världen

Alla länder som är medlemmar i den Europeiska unionen har, i enlighet med artikel 28 i det nuvarande dataskyddsdirektivet, åtminstone en tillsynsmyndighet med uppgiften att utöva tillsyn

över direktivets tillämpning och efterlevnad. En motsvarande skyldighet följer av den nya dataskyddsförordningen, som ska börja tillämpas den 25 maj 2018. Den centrala tillsynsmyndigheten har ofta, men inte alltid, också ett tillsynsansvar över frågor som inom EU regleras på annat sätt än genom dataskyddsdirektivet eller som inte alls regleras av EU. I vilken utsträckning det härutöver förekommer andra tillsynsmyndigheter på området med tillsynsansvar för särskilda frågor varierar. Jämförelser är här svåra och vanskliga att göra, eftersom EU-länderna tillhör delvis olika rättskulturer och den statliga förvaltningsstrukturen kan variera beroende bland annat på om en stat är en förbundsstat eller en enhetsstat.

Vissa iakttagelser kan dock göras. Inte i något land ansvarar en enda central dataskyddsmyndighet för tillsynen över all personuppgiftsbehandling. Särskilda organ för tillsyn över sådan personuppgiftsbehandling som förekommer i säkerhets- och underrättelseverksamhet finns i många medlemsländer, exempelvis i Nederländerna, Belgien, Frankrike och Grekland. Sådana myndigheters befogenheter och uppgifter, och deras gränsdragning mot den centrala dataskyddsmyndigheten, varierar. I Storbritannien finns olika ”inspectors” som utövar tillsyn över säkerhets- och underrättelsetjänsterna. Det finns i många länders parlament också ett särskilt utskott som granskar säkerhets- och underrättelsetjänsternas verksamhet.

Det finns vidare i flera länder särskilda tillsynsmyndigheter för dataskydd inom exempelvis vård och omsorg och inom forskning på människor. Tillsyn över personuppgiftsbehandling inom post- och telekommunikation är ofta en uppgift för den centrala tillsynsmyndigheten. Så är det exempelvis i Frankrike, Italien, Irland, Storbritannien och i de baltiska länderna. Det förekommer emellertid också, t.ex. i Belgien, Ungern och Kroatien, att tillsynen inom detta område på samma sätt som i Sverige utförs av en särskild myndighet, liksom att tillsynsansvaret är delat mellan den centrala tillsynsmyndigheten och en annan, särskild myndighet (så är det t.ex. i Nederländerna, Grekland och Tyskland).

I länder med ett federalt styre eller annars med starkt regionalt självstyre, såsom Tyskland och Spanien, finns ofta en central tillsynsmyndighet på nationell nivå och tillsynsmyndigheter på regional nivå eller delstatsnivå. I Tyskland har inte alla delstater organiserat tillsynen på samma sätt; i några delstater utövar den regionala

myndigheten tillsyn bara över privat verksamhet och i andra över både privat och offentlig.

I t.ex. Kanada, Australien och Sydafrika finns särskilda tillsynsorgan för säkerhets- och underrättelsetjänsterna. I Australien finns härutöver en central tillsynsmyndighet (Office of the Australian Information Commissioner) som på federal nivå utövar tillsyn över privata aktörers och de flesta federala myndigheters personuppgiftsbehandling. På delstatsnivå finns tillsynsmyndigheter som bland annat utövar tillsyn över personuppgiftsbehandling utförd i delstatsmyndigheter. I USA finns flera s.k. Inspectors General för de olika underrättelsetjänsterna, som dock ofta är anställda vid den granskade myndigheten och därför inte utgör samma oberoende och fristående tillsyn som tillsynsmyndigheterna i de europeiska länderna.

8 Våra iakttagelser och slutsatser

8.1 Inledning

Vi har i det föregående redovisat vår kartläggning av dagens tillsyn över behandlingen av personuppgifter. Kartläggningen visar att ett antal myndigheter har tillsynsansvar som avser personuppgiftsbehandling inom mycket varierande verksamheter, i både privat och offentlig regi. Den centrala tillsynsmyndigheten Datainspektionen har ett brett och omfattande tillsynsområde med befogenhet att utöva tillsyn över all personuppgiftsbehandling. Härutöver har en handfull andra myndigheter behörighet att utöva tillsyn över sådan personuppgiftsbehandling som förekommer i vissa särskilda verksamheter. Tillsynen kompletterar eller ersätter här Datainspektionens tillsyn. I vissa av dessa myndigheter utgör sådan tillsyn en stor del av myndighetens verksamhet. Detta är fallet med den tillsyn som utförs av Säkerhets- och integritetsskyddsnämnden (SIN) och Post- och telestyrelsen (PTS). I andra myndigheter, såsom exempelvis Konsumentverket, Inspektionen för vård och omsorg (IVO) och länsstyrelserna är tillsynen över personuppgiftsbehandling en mer begränsad del av den totala verksamheten. I ett fåtal fall är lagstiftningen utformad på ett sådant sätt att ytterligare några myndigheter rent formellt har ett i vart fall teoretiskt tillsynsansvar även över behandling av personuppgifter.

Detta innebär att tillsynsansvaret till stor del redan i dag är samlat i en myndighet. Den kompletterande tillsyn som utförs av andra myndigheter än Datainspektionen avser i de flesta fall klart avgränsade områden som inte ger upphov till några gränsdragningsfrågor. I några fall kan emellertid konstateras att tillsynsansvaret antingen är parallellt, dvs. två myndigheter har behörighet att utöva tillsyn över samma personuppgiftsbehandling, eller att gränsdragningen mellan de olika myndigheternas befogenheter i

några avseenden är oklar. De flesta sådana gränsdragningsproblem är mest teoretiska, dvs. man kan konstatera att ansvarsfördelningen skulle kunna vara oklar i en viss typ av ärenden men frågan har såvitt vi har kunnat finna aldrig uppkommit i praktiken, eller är inte mer komplicerad än att man kunnat lösa den med ett telefonsamtal. Även om myndigheterna löser arbetsfördelningen mellan sig kan ett parallellt tillsynsansvar eller oklarheter när det gäller gränsdragningen dock ibland göra att tillsynen ur allmänhetens perspektiv uppfattas som mindre effektiv och det vara svårt för den enskilde att förstå vart han eller hon ska vända sig med frågor eller klagomål. Om de berörda myndigheterna dessutom inte har samma befogenheter och deras beslut inte har samma rättsföljd eller inte får överklagas på samma sätt, kan också principiella invändningar riktas mot oklarheterna i ansvarsfördelningen. I endast ett fall visar kartläggningen att olika uppfattningar om vem som har ansvaret för tillsynen i praktiken har lett till att tillsyn inte har utförts av någon myndighet.

8.2 Ett omfattande tillsynsområde

Behandling av personuppgifter förekommer i dag inom alla delar av samhället, hos myndigheter, företag och privatpersoner. I takt med den tekniska utvecklingen blir digitala tjänster vanligare, vilket ofta innefattar personuppgiftsbehandling. I tider med ökat fokus på säkerhet och brottsbekämpning ökar också behovet av och kraven på bland annat övervakning som kan innebära att personuppgifter behandlas. Varje enskild individs personuppgifter behandlas i ett mycket stort antal olika situationer i det dagliga livet. Det gäller t.ex. kund- och medlemsuppgifter, uppgifter om när en bil har passerat en betalstation för trängselskatt, upptagningar från övervakningskameror, betalning av parkeringsplatser via mobiltelefonen, inlägg på sociala medier, reklamutskick via e-post och uppgifter i patientjournaler. Till detta kommer myndigheters behandling av bland annat adress- och inkomstuppgifter för exempelvis utbetalning av ekonomiskt stöd eller beräkning av skattskyldighet. En särskilt känslig behandling gäller de brottsbekämpande myndigheternas användning av register, övervakning och andra metoder som innebär att olika personuppgifter behandlas.

Integritetskommittén har gjort en kartläggning över de risker för den personliga integriteten som följer av det moderna informationssamhället.[1] Som en del i redovisningen av denna kartläggning beskriver kommittén en fiktiv familjs dygn och vilka elektroniska spår familjemedlemmarna lämnar efter sig genom bland annat informationsinhämtning på internet, mobiltelefonsamtal, inlägg på sociala medier och arbetsgivares användning av olika former av övervakning av arbetstagarnas aktiviteter. Aktiviteter som är mer eller mindre vanliga i ett modernt informationssamhälle medför enligt kommittén risker för den personliga integriteten genom användning av bland annat s.k. cookies, e-legitimation, sammanhållen journalföring, övervakningskameror, bristfälliga integritetsinställningar och överföring av okrypterad information.

Också på en internationell nivå, inte minst inom EU, pågår en utveckling mot ett ökat gränsöverskridande utbyte av personuppgifter, också här inom både privat och offentlig verksamhet. Frågor om skyddet för den personliga integriteten vid personuppgiftsbehandling är föremål för ett ökat intresse i många delar av världen, och inom EU har ett omfattande reformarbete genomförts på dataskyddsområdet.

Med en så omfattande personuppgiftsbehandling som dagens samhälle kräver är det givetvis viktigt att de personuppgiftsansvariga har tillräcklig kunskap om gällande bestämmelser kring sådan behandling och att det finns en fungerande ordning som verkar för att bestämmelserna följs. Detta behov kan delvis tillgodoses genom en väl fungerande tillsyn, som därmed bidrar till att skyddet för den enskildes personliga integritet stärks. I de fall personuppgifter har behandlats på ett otillåtet sätt kan tillsynen vidare innebära t.ex. att den enskilde får felaktiga uppgifter rättade och tillerkänns kompensation i form av skadestånd, eller att den personuppgiftsansvarige föreläggs att upphöra med en felaktig behandling.

Datainspektionen är i Sverige den myndighet som har det övergripande ansvaret för tillsynen över behandlingen av personuppgifter. Härutöver är myndighetens arbete till stor del inriktad på förebyggande insatser, såsom informationskampanjer, en webbsida med omfattande information om dataskyddsfrågor, kurser för per-

[1] Kartläggningen redovisas i delbetänkandet Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén (SOU 2016:41).

sonuppgiftsombud och personuppgiftsansvariga samt en upplysningstjänst för besvarande av frågor via telefon. Inom Datainspektionen finns en bred kompetens och erfarenhet inom området för personuppgiftsbehandling och integritetsskydd och det övergripande tillsynsansvaret ger goda förutsättningar för överblick och helhetssyn. Datainspektionens uppgift som nationell tillsynsmyndighet enligt det nuvarande dataskyddsdirektivet och myndighetens medverkan i det internationella samarbetet kring personuppgiftsbehandling och skyddet för den personliga integriteten innebär också att det inom myndigheten finns en stor kunskap om EU-rätten och andra internationella rättsliga regleringar kring dataskydd.

De övriga myndigheter som utövar tillsyn över personuppgiftsbehandling gör detta inom avgränsade sakområden. Ett sådant, inom vissa områden, särskilt utpekat tillsynsansvar har ofta motiverats med att den personuppgiftsbehandling som där är föremål för tillsyn utgör en del av och har en naturlig och nära koppling till den verksamhet som i övrigt är föremål för myndighetens ansvarsområde och tillsyn. Detta gäller exempelvis för den tillsyn som utförs av PTS och Konsumentverket. Den personuppgiftsbehandling som är föremål för särskild tillsyn kan vidare avse en verksamhet där det har ansetts att det krävs särskild insikt i och erfarenhet av den granskade verksamheten. Tillsynen är där inriktad på områden som kan ge upphov till särskilda risker från integritetssynpunkt. Detta gäller t.ex. för den tillsyn som utförs av SIN.

Till detta kommer att det kan vara omöjligt att särskilja de åtgärder som innebär att en personuppgift har behandlats från andra åtgärder som också är föremål för en viss myndighets tillsyn. De behandlingsregler i lagen om elektronisk kommunikation som är föremål för tillsyn av PTS avser exempelvis kommunikation som kan, men inte behöver, innehålla personuppgifter som går att koppla till en fysisk person.

8.3 Är det möjligt att samla all tillsyn över behandling av personuppgifter hos en myndighet?

Bedömning: Det är inte möjligt och vore inte heller lämpligt att samla all tillsyn över behandling av personuppgifter hos en myndighet. Det skulle heller inte stärka skyddet för enskildas personliga integritet.

Tillsynen över behandling av personuppgifter är redan i dag till stor del samlad hos en myndighet, Datainspektionen. Datainspektionen bör även i fortsättningen vara den centrala myndigheten när det gäller personuppgiftsbehandling. Vi anser att myndigheten även efter genomförandet av EU:s dataskyddsreform bör behålla sitt nuvarande namn.

För att tillsynen ska bli ännu mera ändamålsenligt utformad och skyddet för den personliga integriteten därmed starkare, kan en viss överföring av tillsynsuppgifter från en tillsynsmyndighet till en annan behöva genomföras. Berörda myndigheter kan också behöva samråda i ökad omfattning. Vi återkommer i kapitel 10 till överväganden om var det finns ett sådant behov.

Våra utredningsdirektiv anger att det i uppdraget ingår att analysera fördelar och nackdelar med att i högre grad än hittills samla tillsynen över behandlingen av personuppgifter hos en myndighet. Det kan synas rimligt att anta att ett ännu mera samlat tillsynsansvar skulle kunna vara en fördel när det gäller effektivitet, resursutnyttjande och enhetlighet i tillsynsarbetet. Om det bara fanns en myndighet med ansvar för tillsynen av den personliga integriteten skulle det onekligen vara tydligt vilken myndighet som bär ansvaret. Det skulle också kunna ses som en fördel för tillsynsobjekten om en mera samlad tillsyn innebar att de skulle slippa bli föremål för tillsyn från olika håll. Att vara föremål för tillsyn tar resurser i anspråk i en granskad verksamhet; uppgifter och material kan behöva tas fram och personal avsättas för att bland annat ta emot tillsynsmyndigheternas representanter.

Som bland annat Statskontoret har betonat är det viktigt att gränssnittet mellan tillsynsmyndigheter med liknande uppgifter blir

tydligt, så att det inte uppkommer otydlighet och överlappande ansvar mellan olika myndigheter.[2]

Enbart utmaningen att formulera tydliga gränssnitt mellan myndigheter med liknande uppgifter utgör dock inte ett tillräckligt skäl för att samla all tillsyn över behandlingen av personuppgifter hos en myndighet. Det är naturligtvis alltid nödvändigt att en myndighets uppgifter är noga preciserade så att det inte råder någon osäkerhet om vad myndigheten har att göra och vilka befogenheter den har. Om man väljer att dela ansvaret för en uppgift mellan olika myndigheter ställs det, mot bakgrund av risken för gränsdragningsproblem, särskilda krav på att det klargörs vilken myndighet som ska göra vad. Samtidigt är givetvis den viktigaste frågan hur tillsynen ska organiseras för att bäst skydda enskildas integritet.

En vanlig frågeställning när det gäller organiseringen av den statliga tillsynen är i vilken utsträckning det bör inrättas en särskild fristående myndighet med uppdraget att utöva tillsyn över en eller flera andra myndigheter. En sådan diskussion tar ofta sin utgångspunkt i distinktionen mellan intern och extern tillsyn, och i viss mån även mellan ordinär och extraordinär tillsyn. Frågan kan då ställas om den tillsyn som redan utförs av exempelvis de extraordinära tillsynsmyndigheterna Riksdagens ombudsmän och Justitiekanslern är tillräcklig, om den granskning som en fristående myndighet utför kan sägas vara mer självständig och oberoende än den som utförs inom den aktuella verksamheten, samt om en ordinär men fristående tillsynsmyndighet kan förväntas bidra till ett ökat förtroende för myndighetens och det allmännas verksamhet.

Förutsättningarna inom det område som är föremål för denna utrednings överväganden är emellertid helt andra. Inom det tillsynsområde som gäller behandling av personuppgifter och skyddet av den personliga integriteten vid sådan behandling finns i dag redan ett antal statliga myndigheter med uppgift att utöva tillsyn. Frågan vi har att ta ställning till är därför vilka fördelar och nackdelar det finns med att samla dessa myndigheters tillsynsuppgifter hos en enda myndighet. Denna fråga inbegriper både mer allmänna överväganden om eventuella fördelar med ett mera samlat tillsynsansvar i allmänhet och, mer specifikt, om det finns några för-

[2] Tänk till om tillsynen – om utformningen av statlig tillsyn, Statskontoret 2012.

delar med att samla de uppgifter som utförs av dagens tillsynsmyndigheter hos en myndighet. Sådana fördelar ska för att vara relevanta i detta sammanhang, i enlighet med våra direktiv, stärka skyddet för den enskildes personliga integritet.

Vi har funnit att Datainspektionen, som redan i dag har ett övergripande och i sak det mest omfattande tillsynsansvaret över personuppgiftsbehandling i både privat och offentlig verksamhet, har en samlad och väl upparbetad erfarenhet och kompetens när det gäller personuppgifts- och integritetsfrågor. Detta ger fördelar i form av effektivitet och kvalitet. Det finns enligt vår bedömning förutsättningar för Datainspektionen att upprätthålla en god överblick över den personuppgiftsbehandling som förekommer i samhället i dag, liksom över utvecklingen inom området för dataskydd och integritet. Vår slutsats är mot den bakgrunden att Datainspektionen, som redan i dag har en tydlig position som den myndighet som har ett övergripande ansvar när det gäller tillsynen över den personliga integriteten, även efter genomförandet av EU:s dataskyddsreform, bör behålla uppgiften att vara den centrala tillsynsmyndigheten när det gäller tillsynen över den personliga integriteten vid behandling av personuppgifter.

Vi har övervägt om det, för att tydliggöra Datainspektionens roll som den centrala tillsynsmyndigheten när det gäller den personliga integriteten, finns skäl att ge myndigheten ett nytt namn. Myndigheten har haft sitt nuvarande namn sedan den inrättades, i samband med att datalagen (1973:289) trädde i kraft. Datalagen ersattes senare av personuppgiftslagen. Det kan möjligen hävdas att namnet är ålderdomligt och inte fullt ut beskriver vad myndigheten gör. Ett tänkbart nytt namn skulle kunna vara Dataskyddsmyndigheten, Integritetsmyndigheten eller Integritetsskyddsmyndigheten. Det nuvarande namnet är å andra sidan mycket välkänt och väl inarbetat, både i Sverige och internationellt. Det viktigaste skälet för ett namnbyte skulle enligt vår bedömning vara om detta kan antas ha betydelse för att enskilda ska veta vilken myndighet man kan vända sig till med frågor och klagomål som gäller personlig integritet. Enligt vår bedömning skulle emellertid ett namnbyte snarare skapa osäkerhet hos allmänheten. Datainspektionen är även ett namn som stämmer väl överens med det namn som motsvarande myndigheter har i flera andra europeiska länder. Namnet speglar även den omständigheten att tillsynsom-

rådet rör behandling av personuppgifter och inte alla former av integritetsskydd. Myndighetens uppdrag omfattar samtidigt också frågor som inte direkt tar sikte på enskildas integritetsskydd. Till detta kan läggas praktiska och ekonomiska konsekvenser som skulle följa med ett namnbyte. Vi anser mot den här bakgrunden att det saknas bärande skäl för att byta ut det väl kända och tydliga namnet Datainspektionen.

Frågan är då om tillsynen skulle bli bättre och skyddet för den enskildes personliga integritet starkare om Datainspektionens tillsyn omfattade all, och inte bara merparten av, den personuppgiftsbehandling som förekommer.

En fördel kunde som redan sagts antas vara att det i alla situationer skulle vara alldeles klart var tillsynsansvaret ligger. Ett exempel på ett tillsynsområde där oklarheter skulle kunna uppkomma är den personuppgiftsbehandling som utförs med stöd av polisdatalagen, både inom den öppna polisen och inom Säkerhetspolisen. Tillsynen är här i dag parallell, dvs. både Datainspektionen och SIN kan utföra tillsyn. Det kan i ett enskilt fall råda osäkerhet om vilken av dessa myndigheter som ska genomföra tillsynsåtgärderna, och det kan vara svårt för en utomstående att förstå varför ansvarsfördelningen i ett enskilt fall blir som den blir. Så utfördes t.ex. tillsynen över det s.k. kringresanderegistret av SIN,[3] medan Datainspektionen inledde ett tillsynsärende om det s.k. kvinnoregistret.[4] I båda fallen rörde det sig om behandling av personuppgifter i den öppna polisens brottsbekämpande verksamhet. De två myndigheterna har också delvis olika befogenheter och det finns olika möjligheter för den som vill överklaga ett beslut beroende på vilken myndighet som har utfört tillsynen. Den parallella tillsynen kan därmed få även andra konsekvenser än att det är otydligt var ansvaret ligger.

Det skulle kunna hävdas att en annan fördel med att samla tillsynen vore att detta kunde ge ännu bättre förutsättningar att skapa en helhetsbild av det flöde av personuppgifter som utbytet av uppgifter mellan olika myndigheter innebär, både inom Sverige och på internationell nivå, i synnerhet inom EU. Utvecklingen går mot

[3] Säkerhets- och integritetsskyddsnämndens ärende med dnr 173-2013, uttalande den 15 november 2013.
[4] Datainspektionens ärende med dnr 2790-2014, beslut den 24 juni 2015.

ett ökat gränöverskridande utbyte av personuppgifter. Det behov av samordning och samarbete med tillsynsmyndigheter i andra medlemsstater i EU som redan är stort kommer att öka ytterligare i betydelse när de nya EU-rättsakterna på dataskyddsområdet börjar tillämpas. Detta gäller både för hanteringen av enskilda tillsynsärenden och inom ramen för det arbete som ska bedrivas i dataskyddsstyrelsen (European Data Protection Board, EDPB). Endast en myndighet kan vara representerad i dataskyddsstyrelsen, och om denna myndighet har det fullständiga tillsynsansvaret även på hemmaplan skulle det kanske kunna bidra till att arbetet i och kommunikationen med styrelsen underlättas. Enligt vår bedömning är detta dock inte något vägande skäl. Redan i dag är det bara Datainspektionen som är representerad i Artikel 29-gruppen, men när en fråga om personuppgiftsbehandling är föremål för gruppens arbete kan det i Sverige i stället vara PTS som är ansvarig tillsynsmyndighet. I sådana situationer samråder myndigheterna med varandra, en ordning som enligt myndigheterna fungerar väl.

De eventuella utmaningarna med dagens ordning och därmed tänkbara fördelar med ett ännu mer samlat tillsynsansvar ska således inte överdrivas. Vår bedömning är att i den mån gränsdragningen mellan två myndigheters tillsynsansvar i ett visst fall inte är helt klar kan en relativt enkel kommunikation och samverkan mellan myndigheterna i de allra flesta fall lösa problemet. Den absoluta merparten av all personuppgiftsbehandling står vidare redan under en enda myndighets tillsyn. Och det finns klara fördelar med ett härutöver delvis delat tillsynsansvar.

Den kartläggning vi har gjort av dagens tillsyn tydliggör att behandling av personuppgifter förekommer i en mycket stor omfattning och i mycket varierande typer av verksamheter. Det är när det gäller viss sådan verksamhet värdefullt och rent av nödvändigt att tillsynen bedrivs av en myndighet som har särskilda expertkunskaper på det område där behandlingen äger rum. Att uppdra åt en och samma myndighet att utöva tillsyn över all personuppgiftsbehandling, oavsett i vilket sammanhang och i vilken verksamhet den förekommer, skulle enligt vår bedömning inte ge ett bättre skydd för enskildas personliga integritet. Man skulle i stället gå miste om fördelarna med att inom vissa för den personliga integriteten särskilt viktiga områden kunna utnyttja expertmyndigheternas särskilda kunskap om de granskade verksamheterna.

Ett lite speciellt men praktiskt exempel kan återigen vara den tillsyn, i vid mening, som blev följden av Dagens nyheters publicering rörande det s.k. kringresanderegistret. Denna uppgiftssamling prövades, ur olika infallsvinklar, av SIN, Åklagarmyndigheten, Justitiekanslern, Riksdagens ombudsmän, Diskrimineringsombudsmannen och polisen som alla genomförde någon form av tillsyn som på olika sätt hade fokus bland annat på frågan om enskildas personliga integritet. I media liksom i den allmänna debatten framfördes av vissa uppfattningen att det var förvirrande och innebar en brist att flera myndigheter i detta fall kom att utöva tillsyn. Det är naturligtvis olyckligt om myndigheterna inte lyckades förklara sina olika uppdrag. Enligt vår bedömning innebar dock dessa olika tillsynsinsatser att de frågor som uppgiftssamlingen väckte kom att utredas på ett bättre och mera allsidigt sätt än vad som hade blivit fallet om endast en myndighet hade varit behörig att utöva tillsyn. Att flera myndigheter utövar tillsyn med olika utgångspunkter kan i vissa fall bidra till att tillsynen blir så fullständig som möjligt.

Ett annat skäl till varför det knappast är möjligt att överlåta all tillsyn till en enda myndighet är att personuppgiftsbehandlingen ibland har en sådan koppling till annat som en tillsynsmyndighet också utövar tillsyn över att det kan vara i det närmaste omöjligt att särskilja den. Som exempel kan här nämnas att en av huvuduppgifterna för PTS är att utöva tillsyn över informationssäkerheten i elektronisk kommunikation, med andra ord att exempelvis se till att meddelanden når mottagaren utan att obehöriga får tillgång till uppgifterna i meddelandet. Vissa sådana meddelanden innehåller personuppgifter medan andra inte gör det. Om all tillsyn över behandling av personuppgifter skulle utföra av endast en myndighet, skulle sådana meddelanden som innebär att personuppgifter behandlas behöva särskiljas från sådana som inte gör det. En sådan åtskillnad av olika meddelanden framstår för det första inte som möjlig att göra och skulle för det andra förutsätta att själva innehållet i meddelandena analyserades, vilket skulle innebära allvarliga betänkligheter ur ett integritetsperspektiv.

Vår utgångspunkt är mot den här bakgrunden att det redan i dag finns en myndighet, Datainspektionen, som har det övergripande och i realiteten också till stor del det faktiska tillsynsansvaret när det gäller behandling av personuppgifter. Härutöver finns några myndigheter som har ett begränsat tillsynsansvar över viss person-

uppgiftsbehandling, ibland i stället för Datainspektionen och ibland parallellt med Datainspektionen, ofta eftersom behandlingen har en stark koppling till den verksamhet som är den andra myndighetens huvuduppgift, och där personuppgiftsbehandlingen dessutom svårligen i ett enskilt tillsynsärende kan särskiljas från annat som där är föremål för tillsyn.

Mot bakgrund av det mycket omfattande tillsynsområdet och de särskilda skäl som ligger bakom den fördelning av ansvar som till viss del förekommer i dag anser vi därför att det inte är möjligt eller ens lämpligt att samla all tillsyn över behandlingen av personuppgifter hos en enda myndighet.

Med detta sagt finns det emellertid skäl att överväga om ett *delvis* mer samlat tillsynsansvar skulle stärka skyddet för den enskildes personliga integritet. Att flytta över vissa tillsynsuppgifter från någon av de andra myndigheterna till Datainspektionen, för att därigenom exempelvis tydliggöra ansvarsfördelningen mellan myndigheterna, undvika risker för överlappande tillsynsinsatser eller åstadkomma en ansvarsfördelning som är bättre anpassad efter de olika myndigheternas uppdrag och verksamhet, skulle kunna vara ett sätt att åstadkomma ett ännu starkare skydd för enskildas personliga integritet.

När vi i vårt arbete har funnit att det finns vissa oklarheter eller andra brister i hur ansvaret för tillsynen är fördelat har vi därför övervägt i vilken utsträckning detta kan avhjälpas på andra sätt än genom att samla all tillsyn i en myndighet. Sådana överväganden tar sikte på de eventuella fördelarna både med att låta Datainspektionen få överta ansvaret för en tillsynsuppgift som myndigheten inte tidigare har haft och att låta Datainspektionen ensam utöva sådan tillsyn som tidigare varit föremål även för en annan myndighets tillsynsinsatser. Vi har också ansett oss oförhindrade att överväga om tillsynen kan förbättras även på andra sätt, exempelvis genom en ökad samverkan mellan tillsynsmyndigheter.

I det följande redovisar vi var vi har funnit att det finns gränsdragningsproblem eller andra brister i hur ansvaret för tillsynen är fördelat som skulle kunna påverka skyddet av den personliga integriteten negativt. I ett kommande kapitel (kapitel 10) lämnar vi förslag på hur sådana brister bör avhjälpas, samtidigt som de krav som ställs i EU:s nya dataskyddsförordning och dataskyddsdirektiv beaktas.

8.4 Vi har funnit vissa brister i dagens ordning

Bedömning: Vi har funnit vissa brister i gränsdragningen mellan Datainspektionen å ena sidan och Post- och telestyrelsen, Säkerhets- och integritetsskyddsnämnden, Inspektionen för vård och omsorg samt Centrala etikprövningsnämnden å den andra.

8.4.1 Inledning

Vi har konstaterat att de oklarheter som kan uppstå när fler än en myndighet ansvarar för tillsynen över en viss fråga kan bestå i att ansvaret är parallellt eller att ansvaret visserligen är uppdelat men att det i praktiken är svårt att dra gränsen mellan respektive ansvarsområde. Sådana oklarheter i ansvarsfördelningen mellan myndigheter kan orsaka praktiska bekymmer för de berörda tillsynsmyndigheterna men kan också skapa osäkerhet hos enskilda och hos andra myndigheter om vem som bär ansvaret. Särskilt hos enskilda kan oklara ansvarsförhållanden och otydliga gränser bidra till en negativ bild av hur effektiv tillsynen är och skapa ett bristande förtroende för hur statsapparaten i stort fungerar. Härutöver kan ett dubbelt tillsynsansvar vara betungande för tillsynsobjekten, som kan behöva medverka – genom att exempelvis ta fram material, ställa personal till förfogande, skapa tillträde till vissa lokaler m.m. – vid flera olika tillsynsinsatser. När det är fråga om parallella tillsynsuppdrag, dvs. där fler än en myndighet kan utöva tillsyn över samma företeelse, finns dessutom en risk för att olika tillsynsinsatser resulterar i olika bedömningar. Det blir då, både för tillsynsobjektet och för andra som läser besluten, oklart vad som ska anses gälla. En särskilt komplicerande fråga är om myndigheter med parallella tillsynsuppdrag har olika befogenheter och olika överklagandebestämmelser.

Samtliga de myndigheter som har ett tillsynsansvar över personuppgiftsbehandling som ersätter eller är parallellt med Datainspektionens har även andra uppgifter. Några myndigheter är renodlade tillsynsmyndigheter, med tillsyn även över annat än personuppgiftsbehandling, hos andra är tillsyn bara en del av många uppgifter. I vissa fall har den tillsynsuppgift som avser personuppgiftsbehandling en nära koppling till myndighetens huvudsakliga uppgifter

och i andra saknas en sådan nära koppling. Som exempel på de senare kan nämnas Finansinspektionen och Naturvårdsverket (se redovisningen av kartläggningen i kapitel 6).

I detta sammanhang finns anledning att nämna ytterligare en fråga som rör Datainspektionens verksamhet. Datainspektionen är tillstånds- och tillsynsmyndighet även enligt inkassolagen (1974:182). Tillsynsverksamheten är här i huvudsak inriktad på andra frågor än behandlingen av personuppgifter, nämligen inkassoföretagens iakttagande av god inkassosed. Datainspektionens tillsyn omfattar enligt 13 § inkassolagen dock inte verksamhet som står under Finansinspektionens tillsyn. Detta gäller inkassoföretag som också ägnar sig åt exempelvis kreditgivning. För enskilda gäldenärer kan det vara svårt att veta vilken myndighet man ska vända sig till för att påtala brister i en inkassoverksamhet och den parallella tillsynen kan medföra risker för olika bedömningar och praxis på inkassoområdet. Dessutom innebär Datainspektionens tillsynsansvar på inkassoområdet, som tar sikte på andra frågor än de som Datainspektionen annars ägnar sig åt, att myndighetens resurser i mindre utsträckning kan ägnas åt integritetsskydd vid behandling av personuppgifter.

8.4.2 Några gränsdragningsfrågor mellan olika tillsynsmyndigheter

Vi har inom ramen för kartläggningen av dagens tillsyn konstaterat att det i några fall förekommer en viss överlappning eller andra typer av oklarheter när det gäller olika myndigheters tillsynsuppdrag såvitt gäller personuppgiftsbehandling. Några ”vita fläckar” i regleringen av tillsynen – i den meningen att det skulle finnas personuppgiftsbehandling som inte omfattas av någon myndighets tillsynsbehörighet – förekommer inte, eftersom Datainspektionen alltid kan utöva tillsyn om inte någon annan myndighet gör det i stället. Som vi har sett förekommer det dock att två myndigheters olika tolkningar av en lagreglering har lett till att ingen av dem har utfört tillsynsinsatser, trots att frågan om behovet av sådana har väckts.

I det följande beskrivs de situationer vi identifierat, tänkbara eller faktiska, där det kan vara oklart vilken av två myndigheter som har ansvaret för tillsynen över personuppgiftsbehandling. Vidare

berörs det faktum att lagstiftningen i vissa fall är utformad så att vissa myndigheter ser ut att ha ett tillsynsansvar som också omfattar personuppgiftsbehandling, trots att detta sannolikt inte varit avsikten.

Post- och telestyrelsen och Datainspektionen

Som ett tydligt exempel på att olika myndigheter kan ha behörighet att utöva tillsyn över olika delar av en och samma verksamhet som innefattar personuppgiftsbehandling, och att gränsen mellan dessa olika delar inte alltid är klar, kan tillsynen över personuppgiftsbehandling vid elektronisk kommunikation nämnas. Som framgår i redovisningen av kartläggningsarbetet är PTS tillsynsmyndighet för bland annat lagen (2003:389) om elektronisk kommunikation (LEK). I den mån denna lag innehåller särskilda bestämmelser om behandling av personuppgifter som avviker från personuppgiftslagen, är LEK tillämplig och PTS är tillsynsmyndighet. Om en viss fråga som rör behandling av personuppgifter vid elektronisk kommunikation inte är särskilt reglerad gäller däremot personuppgiftslagen, för vilken Datainspektionen är tillsynsmyndighet. LEK innehåller exempelvis vissa behandlingsregler, såsom vem som får behandla en personuppgift och för vilket ändamål, men saknar vissa andra, generella behandlingsregler, såsom insynsregler. Sådana finns i stället i personuppgiftslagen, för vilken PTS inte är tillsynsmyndighet. En bestämmelse i LEK om behandling av personuppgifter kan också innehålla begrepp som är centrala i dataskyddslagstiftningen och som också regleras i personuppgiftslagen, såsom begreppet samtycke. Det kan i ett enskilt tillsynsärende i PTS därför ibland uppstå ett behov av samråd med och vägledning av Datainspektionen.

Några av de frågor som regleras i LEK och som därmed faller under PTS tillsynsansvar har inte några tydliga kopplingar till området för elektronisk kommunikation eller utgör en mycket begränsad del av ett förfarande som i övrigt regleras i personuppgiftslagen och som skulle kunna tjäna på att bedömas i ett sammanhang. Utgångspunkten för tillsynen tar här mer renodlat sikte på allmänna dataskyddsrättsliga aspekter än på frågeställningar som är kopplade till området för elektronisk kommunikation. Det gäller bestämmelserna om abonnentförteckningar i 6 kap. 15 och 16 §§

LEK samt den s.k. cookiebestämmelsen i 6 kap. 18 § LEK. Vi återkommer i kapitel 10 till överväganden om vilken myndighet som lämpligast bör ansvara för tillsynen över dessa bestämmelser.

När det gäller relationen och gränsdragningen mellan Datainspektionen och PTS bör i detta sammanhang noteras att grunden för integritetsregleringen i LEK, och därmed också PTS:s yttersta fokus, är vikten av säker kommunikation. Att arbeta med informationssäkerhetsfrågor är också en av PTS:s centrala uppgifter. Att enskildas personliga integritet inte ska kränkas vid behandling av personuppgifter vid sådan kommunikation är bara ett av flera syften med lagen och kraven på säker kommunikation gäller även om inte kommunikationen innehåller personuppgifter. Personuppgiftslagen, inklusive dess krav på säkerhetsåtgärder, gäller å andra sidan just vid behandling av personuppgifter.

Uppdelningen av tillsynsansvar mellan PTS och Datainspektionen medför ibland också utmaningar i arbetet i den s.k. Artikel 29-gruppen, dvs. den grupp av representanter för EU:s medlemsstaters tillsynsmyndigheter som, med stöd av artikel 29 i det nuvarande dataskyddsdirektivet, har inrättats för att öka förutsättningarna för en enhetlig tillämpning av direktivet. Ibland avhandlas där frågor som omfattas av PTS uppdrag men som i vissa andra länder handhas av den centrala tillsynsmyndigheten. PTS finns dock inte representerad i Artikel 29-gruppen, det gör bara Datainspektionen. De två myndigheterna får i sådana situationer samråda med varandra. Samma situation gäller också för andra medlemsstater där tillsynen över personuppgiftsbehandling i elektronisk kommunikation utförs av en annan myndighet än den centrala tillsynsmyndigheten. Det gränsöverskridande samarbetet mellan medlemsstaternas tillsynsmyndigheter kommer att öka när EU:s dataskyddsförordning börjar tillämpas. Artikel 29-gruppen kommer då att ersättas av den europeiska dataskyddsstyrelsen. Endast en myndighet per medlemsstat kommer att vara representerad även i denna.

Säkerhets- och integritetsskyddsnämnden och Datainspektionen

Ett tydligt fall av parallella tillsynsuppdrag är tillsynen över behandling av personuppgifter inom polisens brottsbekämpande verksamhet, där både Datainspektionen och SIN har befogenhet att utöva tillsyn. Att de båda myndigheternas tillsynsuppdrag är parallella innebär att de kan utöva tillsyn över samma personuppgiftsbehandling och pröva den mot samma lagstiftning.

De två myndigheterna uppger att de brukar samråda och bland annat delge varandra sina tillsynsplaner för att undvika likartade tillsynsinsatser. När något oförutsett förhållande uppmärksammas, såsom exempelvis det s.k. kringresanderegistret hos polisen som uppmärksammades i media,[5] har myndigheterna kontakt om var ett tillsynsärende ska inledas. Vilken av myndigheterna som inleder ett tillsynsärende kan i sådana situationer dock närmast te sig bero på slumpen.

Överlappningarna mellan Datainspektionens och SIN:s tillsynsuppdrag gäller i praktiken främst den öppna polisens personuppgiftsbehandling i brottsbekämpande verksamhet. Formellt finns överlappningen av tillsynsansvar även beträffande Säkerhetspolisens personuppgiftsbehandling, men har där ingen praktisk betydelse eftersom Datainspektionen i realiteten inte utövar tillsyn över Säkerhetspolisen.[6]

Den parallella tillsynen förekommer bara i fråga om behandling av personuppgifter i polisens brottsbekämpande verksamhet och bara när det gäller sådan behandling som regleras i polisdatalagen (2010:361)[7] och lagen (2010:362) om polisens allmänna spaningsregister. Personuppgiftsbehandling kan förekomma även i annan verksamhet hos polisen, t.ex. i myndighetens personaladministration. Sådan behandling regleras av personuppgiftslagen och om-

[5] Efter uppgifter i media där det angavs att dåvarande Polismyndigheten i Skåne hade upprättat ett register över flera tusen personer, de flesta romer, granskades saken av SIN. Granskningarna visade att det fanns allvarliga brister vid personuppgiftsbehandlingen i uppgiftssamlingar inom polisens kriminalunderrättelseverksamhet. SIN:s uttalande 2013-11-15 med anledning av tillsynen finns tillgängligt på SIN:s webbplats på följande adress: http://www.sakint.se/Uttalande-Skanepolisens-personuppgiftsbehandling.pdf

[6] Säkerhetspolisen samråder dock även med Datainspektionen enligt 2 § polisdataförordningen (2010:1155) när myndigheten ska införa eller ändra i it-system av större omfattning eller med särskilda risker för intrång i den personliga integriteten.

[7] När det gäller Säkerhetspolisen ska SIN:s tillsyn också avse behandling enligt den förra polisdatalagen (1998:622).

fattas bara av Datainspektionens tillsyn. Detsamma gäller behandling av personuppgifter enligt exempelvis lagarna om belastnings- och misstankeregister.

SIN saknar flera av de befogenheter som Datainspektionen har. SIN har rätt att på begäran få del av uppgifter och att få biträde av de myndigheter som omfattas av tillsynen[8] men kan inte med bindande verkan besluta om rättelse av eller förbud att fortsätta med en felaktig personuppgiftsbehandling. I stället ska SIN anmäla felaktigheter till andra myndigheter, bland annat till Datainspektionen. Nämndens beslut kan inte heller överklagas. Det innebär exempelvis att om Datainspektionen och SIN i varsitt ärende skulle göra samma bedömning beträffande en viss typ av personuppgiftsbehandling, men Datainspektionens beslut efter ett överklagande ändras av domstol, så uppkommer frågan hur man ska se på SIN:s uttalande.

Inspektionen för vård och omsorg – Datainspektionen

Inspektionen för vård och omsorg (IVO) utövar tillsyn över vård och omsorg och har patientsäkerhet som sitt huvudsakliga fokus. Både IVO och Datainspektionen kan utöva tillsyn över att patientdatalagen, som innehåller bestämmelser om personuppgiftsbehandling, följs. Kartläggningen har visat att det finns en risk för att de båda myndigheterna utövar tillsyn över samma frågor, och att de därvid kan fatta beslut med olika innebörd. Datainspektionen och Socialstyrelsen, som innan IVO bildades var den myndighet som hade motsvarande tillsynsansvar, hade tidigare en överenskommelse som innebar att Socialstyrelsen, om den i sin tillsyn stötte på frågeställningar om behandling av personuppgifter, skulle överlämna frågan till Datainspektionen. Någon sådan överenskommelse finns inte längre och myndigheterna har, enligt vad som framkommit vid våra kontakter med dem, olika uppfattning i frågan om huruvida det föreligger gränsdragningssvårigheter. Datainspektionen anser att de båda myndigheternas tillsynsbefogenheter på området för dataskydd inom vård och omsorg, såsom de har

[8] Också myndigheter som inte omfattas av tillsynen är skyldiga att på begäran lämna upplysningar till SIN, 4 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

kommit att formuleras, i viss mån är överlappande, och att det heller inte är möjligt att dra en skarp gräns mellan dem. För att undvika negativa konsekvenser av dessa oklarheter menar Datainspektionen med hänvisning till de båda myndigheternas olika kompetensområden att IVO, vars tillsyn ska avse hur vård och omsorg bedrivs, bör samråda med eller överlämna ärenden till Datainspektionen när IVO i tillsynsverksamheten uppmärksammar förhållanden som kan innebära att personuppgifter har behandlats på ett otillåtet sätt. Datainspektionen menar att IVO inte har tillräcklig erfarenhet på dataskyddsområdet och att det finns en risk för felaktiga bedömningar och beslut, samt för att IVO och Datainspektionen på varsitt håll meddelar beslut med motstridig innebörd. IVO menar å sin sida att det inte föreligger något gränsdragningsproblem eller överlappande tillsynsansvar eftersom de båda myndigheterna har olika fokus, patientsäkerhet respektive integritet. Därmed finns det enligt IVO inget behov av samråd, överlämnande av ärenden eller överenskommelser.

Centrala etikprövningsnämnden – Datainspektionen

När det gäller sådan behandling av personuppgifter som förekommer i forskning och som omfattas av lagen (2003:460) om etikprövning av forskning som avser människor (etikprövningslagen) råder det viss oenighet om vilken myndighet som i olika fall ska utöva tillsyn, Centrala etikprövningsnämnden eller Datainspektionen. De två myndigheterna har gjort olika tolkningar av lagens reglering av att nämnden ska utöva tillsyn endast i den mån tillsynen inte faller inom en annan myndighets tillsynsområde. Förarbetena hänvisar i detta sammanhang till bland annat Datainspektionen.[9]

Centrala etikprövningsnämnden menar att lagtexten och dess förarbeten innebär att nämnden inte kan utöva någon tillsyn över personuppgiftsbehandling inom den forskning som omfattas av etikprövningslagen, eftersom förarbetena till etikprövningslagen hänvisar till att det är Datainspektionen som har befogenhet att utöva sådan tillsyn. Datainspektionen å sin sida menar att detta är en alltför långtgående tolkning av förarbetsuttalandena. Det måste

[9] Prop. 2002/03:50 s. 163 f.

enligt Datainspektionen ankomma på Centrala etikprövningsnämnden att utöva tillsyn över frågor som rör forskningen ifråga, såsom att granska om forskningen är etikprövad och om den i så fall bedrivs i enlighet med etikprövningsbeslutet. Sådan granskning tar sikte på forskningens men också på personuppgiftsbehandlingens förenlighet med etikprövningslagen. Det innebär att behandling av personuppgifter enligt Datainspektionen kan ingå som en del av nämndens tillsyn. Om det däremot gäller att granska om den utförda personuppgiftsbehandlingen är förenlig med personuppgiftslagen anser sig Datainspektionen vara den myndighet som bör utöva tillsyn.

Oklarheterna har i fråga om personuppgiftsbehandlingen inom sådan forskning som omfattas av etikprövningslagen i några fall inneburit att ingen av myndigheterna har ansett sig kunna utföra tillsyn. Centrala etikprövningsnämnden har överlämnat ärenden till Datainspektionen, som i sin tur inte heller har ansett sig vara rätt myndighet att utöva tillsyn. Konsekvensen av detta har blivit att någon tillsyn inte har utförts.

Myndigheten för samhällsskydd och beredskap – Datainspektionen

Myndigheten för samhällsskydd och beredskap (MSB) har vissa uppgifter som tangerar Datainspektionens, på området för informationssäkerhet. Frågor om informationssäkerhet är en naturlig del av MSB:s uppdrag, men är också en fråga för Datainspektionen eftersom personuppgiftslagen innehåller bestämmelser om säkerheten vid behandling av personuppgifter. MSB är inte en tillsynsmyndighet,[10] och dess uppdrag och verksamhet omfattas därför inte av vårt utredningsuppdrag. Vi anser trots detta att det finns skäl att här påpeka att det finns ett visst mått av överlappande ansvar inom området för informationssäkerhet. Detta gäller inte minst när EU:s nya dataskyddsförordning, som bland annat innehåller bestämmelser om rapportering av s.k. personuppgifts-

[10] Utredningen NISU 2014 har i betänkandet Informations- och cybersäkerhet i Sverige – strategi och åtgärder för säker information i staten (SOU 2015:23) föreslagit att MSB ska få i uppdrag att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet.

incidenter,[11] ska börja tillämpas. Det kan finnas anledning att i ett annat sammahang se över ordningen för rapporteringen och andra frågor som gäller relationen mellan MSB och Datainspektionen.

Myndigheter som har ett tillsynsuppdrag som till synes omfattar även personuppgiftsbehandling

Vår kartläggning har slutligen visat att lagstiftningen i flera fall är utformad på ett sådant sätt att några myndigheter, som har i uppdrag att utöva tillsyn över efterlevnaden av en lag, därigenom också ges ett i vart fall teoretiskt uppdrag att utöva tillsyn även över behandlingen av personuppgifter. Såvitt vi har kunnat klargöra är de aktuella myndigheterna ofta inte ens medvetna om att lagstiftningen kan tolkas på ett sådant sätt, och de tillsynsinsatser som faktiskt utförs avser uteslutande andra frågor.

Det är här fråga om lagar som innehåller bestämmelser om personuppgiftsbehandling som ska ersätta eller komplettera bestämmelser i personuppgiftslagen, och som slår fast att en viss myndighet ska utöva tillsyn över att lagens bestämmelser följs. Som exempel kan nämnas Naturvårdsverkets tillsynsansvar enligt lagen (2004:1199) om utsläppsrätter och Finansinspektionens tillsynsansvar enligt lagen (2005:405) om försäkringsförmedling och lagen (2010:751) om betaltjänster. Det finns också föreskrifter som innebär att en myndighet pekas ut både som tillsynsmyndighet och som personuppgiftsansvarig för samma behandling. Detta gäller exempelvis Statens energimyndighet i förordningen (2011:1480) om elcertifikat och Skogsstyrelsen i skogsvårdslagen (1979:429.

[11] S.k. personuppgiftsincidenter (säkerhetsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats) ska enligt artikel 33 i förordningen utan onödigt dröjsmål anmälas till tillsynsmyndigheten.

9 Anpassningar med anledning av EU:s dataskyddsreform

9.1 Inledning

I utredningens direktiv anges att vi ska förhålla oss till den pågående översynen av EU:s dataskyddsreglering och så långt som möjligt lämna de förslag som behövs för att en svensk tillsynsmyndighet ska kunna fullgöra de uppgifter som kan bli resultatet av den översynen. Sedan direktiven beslutades har reformarbetet fortsatt och både den nya allmänna dataskyddsförordningen[1] och ett nytt direktiv om skydd för personuppgifter på det brottsbekämpande området[2] har antagits av Europaparlamentet och rådet. Förordningen ska börja tillämpas den 25 maj 2018 och direktivet ska vara implementerat senast den 6 maj 2018. Både förordningen och direktivet innehåller nya och utvidgade regleringar som gäller de nationella tillsynsmyndigheterna.

Regeringen beslutade den 25 februari och den 17 mars 2016 om två utredningsdirektiv med anledning av de nya rättsakterna.

En särskild utredare har fått i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som förordningen ger anledning till (dir. 2016:15, Ju 2016:04). Utredaren ska bland annat lämna förslag till upphävande av personuppgiftsregleringen och till författningsbestämmelser som kompletterar dataskyddsförordningen, utreda om det finns behov av

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (i detta betänkande kallat dataskyddsförordningen).

[2] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter (i detta betänkande kallat [det nya] dataskyddsdirektivet).

generella bestämmelser för personuppgiftsbehandling utanför EU-rättens tillämpningsområde samt analysera vilka bestämmelser som behövs om bland annat administrativa sanktionsavgifter och behandling av känsliga personuppgifter. Vissa delar av uppdraget rör anpassningar med anledning av förordningens bestämmelser om tillsynsmyndigheter. Utredningen, som har antagit namnet Dataskyddsutredningen, ska redovisa sitt uppdrag senast den 12 maj 2017.

Vidare har en särskild utredare fått i uppdrag att föreslå hur det nya dataskyddsdirektivet ska genomföras i svensk rätt (dir. 2016:21, Ju 2016:06). Utredaren ska bland annat analysera hur svensk rätt förhåller sig till direktivet och lämna förslag till en ny ramlagstiftning med bestämmelser om skydd för personuppgifter inom direktivets tillämpningsområde. En allmän utgångspunkt för utredaren är att sträva efter lösningar som ansluter till nuvarande principer och systematik i bland annat polisdatalagen (2010:361), åklagardatalagen (2015:433) och domstolsdatalagen (2015:728). Utredaren har också vissa uppgifter som rör direktivets reglering av de nationella tillsynsmyndigheterna. Utredningen, som har antagit namnet Utredningen om 2016 års dataskyddsdirektiv, ska genom ett delbetänkande senast den 1 april 2017 redovisa bland annat den del av uppdraget som rör tillsyn. Uppdraget ska slutredovisas senast den 30 september 2017.

När det gäller frågor som rör den eller de tillsynsmyndigheter som Sverige liksom alla andra medlemsstater måste ha för att övervaka tillämpningen av förordningen respektive direktivet finns det beröringspunkter mellan vår utredning och de två nya utredningarna. Regeringen har i direktiven till dessa utredningar preciserat ansvarsfördelningen så att vi ska ansvara för sådana anpassningsfrågor som rör vilken myndighet som ska utses till nationell tillsynsmyndighet enligt rättsakterna och representera övriga svenska tillsynsmyndigheter i Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB), den nationella tillsynsmyndighetens organisation och utnämningen respektive avsättandet av ledamöter i myndigheten, samt myndighetens resurser och därtill anknytande frågor. Vi ska även överväga om den nationella tillsynsmyndigheten bör ges ytterligare befogenheter utöver de som följer av dataskyddsförordningens artikel 58 samt analysera vilket utrymme och behov det finns av regler om exempelvis myndighetens uppgifter i dess instruktion.

Våra överväganden i de nu angivna frågorna bygger på den kunskap och de förhållanden som är kända i dag. De två nämnda utredningarna kan ha anledning att på nytt överväga de frågor som omfattas av vårt uppdrag om det visar sig finnas behov härav, som ett resultat av de ställningstaganden de gör när det gäller vilka anpassningar som är nödvändiga med anledning av förordningen och direktivet.

9.2 Bakgrund

9.2.1 Det nuvarande dataskyddsdirektivet

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i 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 behandling av det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, samt att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Dataskyddsdirektivet gäller inte för behandling av personuppgifter på områden som faller utanför gemenskapsrätten, t.ex. allmän säkerhet, försvar och nationell säkerhet.

Dataskyddsdirektivet har i Sverige genomförts huvudsakligen genom personuppgiftslagen (1998:204). Personuppgiftslagen följer i princip dataskyddsdirektivets struktur och innehåller liksom direktivet bestämmelser om bland annat personuppgiftsansvar, grundläggande krav för behandling av personuppgifter, information till den registrerade, skadestånd och straff. Personuppgiftslagen är tillämplig även utanför EU-rättens område och gäller både för myndigheter och enskilda som behandlar personuppgifter. Härutöver finns en stor mängd övriga bestämmelser i svensk rätt som reglerar behandlingen av personuppgifter, framför allt i olika typer av myndighetsspecifik lagstiftning. Personuppgiftslagen kompletteras vidare av bestämmelser i personuppgiftsförordningen (1998:1191), som pekar ut Datainspektionen som Sveriges nationella tillsynsmyndighet enligt bland annat direktivet.

Direktivet och den svenska lagstiftning som rör behandling av personuppgifter har närmare beskrivits i kapitel 3.

9.2.2 Dataskyddsrambeslutet

Dataskyddsdirektivets allmänna reglering om behandling av personuppgifter gäller inte på området för polissamarbete och straffrättsligt samarbete inom EU. Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) är tillämpligt på uppgifter som överförs eller görs tillgängliga mellan medlemsstater och EU-organ och vissa informationssystem. Rambeslutet gäller däremot inte för rent nationell personuppgiftsbehandling. I Sverige påverkas främst Polismyndigheten, Kustbevakningen, Åklagarmyndigheten, Skatteverket och Tullverket av rambeslutet.

Vid genomförandet av dataskyddsrambeslutet i Sverige bedömdes de flesta av rambeslutets artiklar redan motsvaras av bestämmelser i svensk rätt. De kompletterande bestämmelser som krävdes är genomförda i en särskild lag, lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

9.2.3 EU:s dataskyddsreform

Europaparlamentet och rådet antog den 27 april 2016 en ny allmän dataskyddsförordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsförordningen). Samtidigt antogs ett nytt direktiv om personuppgiftsbehandling i brottsbekämpande verksamhet (det nya dataskyddsdirektivet).

Dataskyddsförordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta det nuvarande dataskyddsdirektivet. Förordningen är direkt tillämplig i medlemsstaterna men både förutsätter och möjliggör vissa kompletterande nationella bestämmelser. I Sverige innebär detta bland annat att personuppgiftslagen måste upphävas och att en kompletterande generell reglering till förordningen behöver tas fram. Det

huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. Förordningen ska börja tillämpas den 25 maj 2018.

Från dataskyddsförordningens tillämpningsområde undantas enligt artikel 2 behandling av personuppgifter som

- utgör ett led i en verksamhet som inte omfattas av unionsrätten,
- medlemsstaterna utför när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken,
- en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll, eller
- behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Härutöver finns i förordningen bestämmelser om ytterligare undantag, t.ex. för registerföring i små och medelstora företag och för personuppgiftsbehandling för forsknings- och arkivändamål.

När det gäller personuppgiftsbehandling i brottsbekämpande verksamhet ska i stället det nya dataskyddsdirektivet tillämpas. Direktivet, som ska vara implementerat senast den 6 maj 2018, innehåller många förpliktelser för medlemsstaterna som är av samma slag som de som följer av det nuvarande rambeslutet. Det innehåller emellertid också några nyheter, såsom en delvis ny och mer detaljerad reglering om rättigheter för enskilda och om skyldigheter för personuppgiftsansvariga eller biträden avseende exempelvis datasäkerhet, dokumentation och loggning, konsekvensanalyser och förhandssamråd med tillsynsmyndigheten samt regler om underrättelser vid s.k. personuppgiftsincidenter.

Både förordningen och direktivet innehåller också mer detaljerade bestämmelser om de nationella tillsynsmyndigheterna än den nuvarande regleringen. De bestämmelser som omfattas av vårt uppdrag behandlas i de följande avsnitten i detta kapitel.

9.3 Dataskyddsförordningens och det nya dataskyddsdirektivets regleringar om de nationella tillsynsmyndigheterna

9.3.1 Inledning

Dataskyddsförordningen baseras till stor del på det nuvarande dataskyddsdirektivets struktur och innehåll men innebär även en rad nyheter, såsom en utökad informationsskyldighet, administrativa sanktionsavgifter och inrättandet av Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB). Ett flertal av nyheterna avser vidare regleringen av de nationella tillsynsmyndigheterna. Dataskyddsförordningens och det nya dataskyddsdirektivets reglering av tillsynsmyndigheternas roll, organisation och uppgifter är mer detaljerad än motsvarande reglering i det nuvarande dataskyddsdirektivet och dataskyddsrambeslutet.

Dataskyddsförordningen förpliktar de nationella tillsynsmyndigheterna i medlemsstaterna att samarbeta med och bistå varandra. Detta innebär bland annat skyldigheter att samråda och utbyta information. Vidare möjliggör, och ibland förutsätter, förordningen gemensamma insatser och utredningar där personal från olika medlemsstaters tillsynsmyndigheter deltar, liksom en överföring av befogenheter från en tillsynsmyndighet i en medlemsstat till tillsynsmyndigheter i andra medlemsstater som är involverade i samma insats.

En förordnings bestämmelser gäller direkt i medlemsstaterna utan krav på nationella lagstiftningsåtgärder. Vissa frågor kan dock i och för sig vara reglerade genom en förordning men kan härutöver tillåta viss ytterligare nationell reglering. Detta gäller för dataskyddsförordningens reglering om bland annat tillsynsmyndighetens befogenheter i artikel 58.[3] Det förekommer också att dataskyddsförordningen inte bara möjliggör utan förutsätter viss nationell lagstiftning. Förordningens artikel 54 anger att medlemsstaterna *i lag* ska reglera bland annat tillsynsmyndighetens

[3] Av artikel 58.6 i förordningen följer att medlemsstaterna i sin nationella lagstiftning får föreskriva att deras tillsynsmyndigheter ska ha ytterligare befogenheter utöver dem som räknas upp i förordningen. Utövandet av dessa befogenheter får dock inte påverka den effektiva tillämpningen av förordningens föreskrifter om tillsynsmyndigheternas samarbete och den enhetliga tillämpningen av förordningen.

inrättande, de kvalifikationer som krävs för att någon ska utnämnas till ledamot av tillsynsmyndigheten och förfarandet för utnämning av tillsynsmyndigheternas ledamöter. Av förordningens preambel följer emellertid att när det i förordningen hänvisas till en rättslig grund eller lagstiftningsåtgärd, inte nödvändigtvis avses en lagstiftningsakt antagen av ett parlament. En rättslig grund eller lagstiftningsåtgärd bör dock vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den.[4] Förordningen och direktivet medger enligt vår mening därmed reglering både i lag beslutad av riksdagen och i förordning beslutad av regeringen.

Även det nya dataskyddsdirektivet innehåller motsvarande detaljerade bestämmelser om de nationella tillsynsmyndigheterna, som till stor del är identiska med förordningens. Ett EU-direktiv är emellertid inte direkt tillämpligt i medlemsstaterna utan förutsätter att medlemsstaterna genomför regleringen i nationell rätt. Den nämnda pågående Utredningen om 2016 års dataskyddsdirektiv har i uppdrag att överväga hur direktivet ska genomföras i svensk rätt. I den utredningens uppdrag ingår bland annat att överväga hur direktivets förpliktelser ska genomföras när det gäller bestämmelserna om tillsyn, med undantag för de frågor om organisation, utnämning respektive avsättande av ledamöter samt resurser och anknytande frågor som tas om hand av vår utredning.

I det följande presenteras våra överväganden med anledning av de regleringar som omfattas av vårt uppdrag.

[4] Beaktandesats (41) i dataskyddsförordningens preambel. Motsvarande beaktandesats finns i direktivet (33).

9.3.2 Ansvarig tillsynsmyndighet och representation i dataskyddsstyrelsen

Bedömning: Svensk rätt uppfyller dataskyddsförordningens och det nya dataskyddsdirektivets krav på att tillsynsmyndigheten ska vara fullständigt oberoende. Tillsynsmyndigheten bör inrättas genom en bestämmelse i en förordning beslutad av regeringen.

Förslag: Datainspektionen ska utses till svensk tillsynsmyndighet enligt dataskyddsförordningen och det nya dataskyddsdirektivet. Detta, och myndighetens deltagande i dataskyddsstyrelsens arbete, ska regleras i Datainspektionens myndighetsinstruktion.

Förordningen och direktivet

Av artikel 28 i det nuvarande dataskyddsdirektivet följer att medlemsstaterna ska utse en eller flera myndigheter som har till uppgift att inom medlemsstatens territorium övervaka tillämpningen av de bestämmelser som följer av direktivet. Sverige har genom 2 § personppgiftsförordningen (1998:1191) slagit fast att det är Datainspektionen som är tillsynsmyndighet enligt personuppgiftslagen, som är den lag som till största delen införlivar det nuvarande dataskyddsdirektivet i svensk rätt.

Av både dataskyddsförordningen och det nya dataskyddsdirektivet följer att varje medlemsstat ska utse en eller flera myndigheter att ansvara för tillsynen över tillämpningen av förordningen respektive direktivet, i syfte att skydda enskildas rättigheter vid behandlingen av personuppgifter och för att möjliggöra det fria flödet av sådana uppgifter (artikel 51.1 i förordningen och artikel 41.1 i direktivet). Detta motsvarar alltså vad som gäller enligt det nuvarande direktivet.

En tillsynsmyndighet ska enligt båda rättsakterna vara fullständigt oberoende i utförandet av de uppgifter och utövandet av de befogenheter som den anförtrotts i rättsakterna. Dess ledamöter ska stå fria från utomstående påverkan och varken begära eller ta emot instruktioner av någon. Ledamöterna ska vidare avstå från alla

handlingar och all annan yrkesverksamhet som står i strid med tjänsteutövningen. Medlemsstaterna ska se till att varje tillsynsmyndighet har sådana resurser, lokaler och infrastruktur som behövs för att den ska kunna utföra sina uppgifter och utöva sina befogenheter. Myndigheterna ska vidare välja och förfoga över sin egen personal, som bara ska ta instruktioner från myndighetsledningen, och myndigheterna ska vara föremål för finansiell kontroll utan att detta påverkar myndighetens oberoende. Myndigheterna ska förfoga över en egen, offentlig årsbudget. Den nationella tillsynsmyndighet som utses ska vidare ha angivna uppgifter och befogenheter och dess ledamöter ska utnämnas och får avsättas på ett sätt som överensstämmer med rättsakterna.

För att säkerställa och underlätta ett samarbete mellan medlemsstaternas tillsynsmyndigheter, och för att garantera en konsekvent tillämpning av dataskyddsförordningen i EU ska en europeisk dataskyddsstyrelse inrättas (European Data Protection Board, EDPB). Styrelsen ska ersätta Arbetsgruppen för uppgiftsskydd, den s.k. Artikel 29-gruppen, och ges en mer central roll. De nationella tillsynsmyndigheterna ska bland annat vara skyldiga att samråda med dataskyddsstyrelsen innan de vidtar åtgärder som kan få konsekvenser i andra medlemsstater. Om det i en medlemsstat finns fler än en tillsynsmyndighet ska en av dem utses att representera de andra i dataskyddsstyrelsen (artikel 51.3 i förordningen och artikel 41.4 i direktivet).

Vårt förslag i frågan om det bör inrättas en ny myndighet med ett samlat ansvar för tillsynen över behandling av personuppgifter

Vi har i kapitel 8 redovisat våra överväganden i frågan om det bör inrättas en ny myndighet med ett samlat ansvar för tillsynen över personuppgiftsbehandling. Vi har funnit att den nuvarande ordningen, som innebär att Datainspektionen är central tillsynsmyndighet med det huvudsakliga ansvaret för tillsynen över behandling av personuppgifter och att några ytterligare myndigheter har begränsade tillsynsuppgifter för vissa särskilda sakområden, är den ordning som bäst kan skydda enskildas integritet och att den inte bör och inte heller kan ersättas med en ordning där all tillsyn utövas av en myndighet.

Detta innebär att Datainspektionen med våra förslag ska finnas kvar som central tillsynsmyndighet, med i allt väsentligt samma uppgifter som i dag. Vid sidan av Datainspektionens tillsyn ska viss tillsyn även i fortsättningen bedrivas av några andra myndigheter. Vi återkommer i kapitel 10 till frågan om det finns anledning att inom ramen för denna tillsynsstruktur, och med beaktande av kraven i de nya EU-rättsakterna, på nationell nivå göra några ändringar i tillsynsansvaret för olika myndigheter, i syfte att ytterligare tydliggöra gränsdragningen mellan olika myndigheters tillsynsuppdrag, skapa en mer ändamålsenlig tillsyn och stärka skyddet för den personliga integriteten.

Gällande svensk ordning för en oberoende förvaltning

Den eller de myndigheter som utses att övervaka tillämpningen av dataskyddsförordningen och det nya dataskyddsdirektivet måste vara fullständigt oberoende i utförandet av de uppgifter och utövandet av de befogenheter som den anförtrotts i rättsakterna. I kravet på att en tillsynsmyndighet ska vara ”fullständigt” oberoende ligger både att den ska vara fristående och självständig i förhållande till den verksamhet den är satt att övervaka och att det inte heller får förekomma någon påverkan, direkt eller indirekt, från något annat håll, såsom från staten.[5]

Den svenska förvaltningsorganisationen, med ett relativt litet regeringskansli och med förvaltningsmyndigheter som är fristående i förhållande till regeringen och Regeringskansliet, skiljer sig från sina motsvarigheter i de flesta andra europeiska länder, där förvaltningen i stället ofta är en del av regeringens kansli och där den ansvariga ministern kan utöva ett direkt bestämmande över myndigheterna.

De svenska förvaltningsmyndigheternas självständiga ställning och oberoende i beslutsfattandet garanteras i regeringsformen. Att förvaltningsmyndigheterna lyder under regeringen (12 kap. 1 §) innebär att föreskrifter från regeringen ska riktas till myndigheten, inte till enskilda tjänstemän.[6] Regeringens styrning av myndighe-

[5] Se t.ex. EU-domstolens dom i mål C-518/07.
[6] SOU 1972:15 s. 195 och SOU 2008:125 s. 351. Se också Holmberg m.fl., Grundlagarna (3 uppl. 2012), s. 556.

terna är vidare begränsad, främst genom bestämmelsen i 12 kap. 2 § som slår fast att ingen myndighet, inte heller riksdagen eller en kommuns beslutande organ, får bestämma hur en förvaltningsmyndighet i ett särskilt fall ska besluta i ett ärende som rör myndighetsutövning mot en enskild eller mot en kommun eller som rör tillämpningen av lag. Riksdagen får heller inte fullgöra förvaltningsuppgifter i vidare mån än vad som följer av grundlag eller riksdagsordningen (12 kap. 3 §). Vidare följer principen om maktutövningens lagbundenhet av 1 kap. 1 § regeringsformen som säger att den offentliga makten utövas under lagarna. Denna princip gäller även regeringen i styrningen av förvaltningen. Saklighetskravet i 1 kap. 9 § innebär vidare att förvaltningsmyndigheter och andra som fullgör offentliga förvaltningsuppgifter i sin verksamhet ska beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet.

I lagen (1994:260) om offentlig anställning (LOA) finns bestämmelser som förbjuder förtroendeskadliga bisysslor och i förvaltningslagen (1986:223) finns bestämmelser om jäv.

En ytterligare skärpning av förvaltningens oberoende ligger i den begränsning av regeringens roll som beslutsfattare i enskilda ärenden som har genomförts under senare decennier. Många ärendetyper som tidigare avgjordes av regeringen har numera delegerats till förvaltningsmyndigheter med möjlighet att överklaga deras beslut till förvaltningsdomstol.

Regeringen får därmed inte styra förvaltningsmyndigheterna genom att påverka dem i handläggningen av ärenden. Styrningen får bara ske på ett generellt plan och genom förordningar och särskilda regeringsbeslut. Finansmakten och regeringens regleringsbrev är en annan form av tillåten styrning. Kontakter mellan Regeringskansliet och förvaltningen har ansetts vara viktiga inslag i en effektiv förvaltning, men bör inskränkas till ett informations- och kunskapsutbyte.[7]

Riksrevisionen granskar verksamheten i de statliga förvaltningsmyndigheterna. Granskningen tar bland annat sikte på om myndigheterna använder statliga medel på ett avsett och effektivt sätt och om deras årsredovisningar är tillförlitliga och korrekta. Varje svensk förvaltningsmyndighet förfogar över en egen, offentlig årsbudget.

[7] Se bl.a. prop. 2009/10:175, s. 101 f. och bet. 2009/10:FiU38.

EU-domstolen har i mål mot Tyskland, Österrike och Ungern haft vissa synpunkter på dataskyddsmyndigheternas oberoende enligt det nuvarande dataskyddsdirektivet, där bland annat frågan om deras relation till regeringen varit aktuell. Förhållandena var i de fallen dock helt andra än i Sverige, med sådan statlig kontroll av tillsynsmyndighetens beslutsfattande i enskilda fall att det inte kunde uteslutas att myndigheten påverkades av politiska hänsyn respektive den omständigheten att regeringen och tillsynsmyndigheten delvis hade gemensam personal.[8]

Våra överväganden

Den svenska förvaltningsmodellen innebär starka och till största delen grundlagsfästa garantier för oberoende i beslutsfattandet för förvaltningsmyndigheter under regeringen. De kommande EU-rättsakternas krav på tillsynsmyndighetens oberoende uppfylls enligt vår mening utan tvekan med den svenska ordningen. Det kan tilläggas att redan det nu gällande dataskyddsdirektivet ställer krav på att tillsynsmyndigheterna ska vara fullständigt oberoende.

Datainspektionen är i Sverige den centrala tillsynsmyndigheten på dataskyddsområdet, med ett brett mandat att utöva tillsyn över i stort sett all behandling av personuppgifter. Datainspektionen motsvarar förordningens och direktivets krav på oberoende och har de befogenheter som krävs. Vi föreslår därför att Datainspektionen utses till tillsynsmyndighet enligt dataskyddsförordningen respektive det nya dataskyddsdirektivet. Datainspektionen ska därmed också delta i arbetet i dataskyddsstyrelsen, vilket bör anges i myndighetens instruktion.

När det gäller sådan personuppgiftsbehandling som utförs inom direktivets tillämpningsområde konstaterar vi att tillsyn i Sverige utförs även av Säkerhets- och integritetsskyddsnämnden (SIN). Denna myndighet saknar emellertid flera av de befogenheter som enligt direktivet är nödvändiga för en tillsynsmyndighet, såsom exempelvis att med bindande verkan kräva rättelse av en felaktig behandling. SIN kan därmed inte i sin nuvarande utformning utgöra en nationell tillsynsmyndighet enligt direktivet. Ingenting

[8] Mål C-518/07 (Tyskland), C-614/10 (Österrike) och C-288/12 (Ungern).

hindrar dock enligt vår mening att Datainspektionens tillsyn på nationell nivå kompletteras av ytterligare myndigheters tillsyn, förutsatt att detta inte begränsar Datainspektionens tillsynsmandat. Vi återkommer i kapitel 10 till frågor som rör Datainspektionens och SIN:s tillsyn över personuppgiftsbehandling inom polisens brottsbekämpande verksamhet.

Datainspektionen är, liksom de flesta svenska statliga förvaltningsmyndigheter, en myndighet under regeringen. Vi finner, mot den ovan redovisade beskrivningen av de svenska förvaltningsmyndigheternas självständiga ställning, ingen anledning att föreslå någon förändring av den ordningen med anledning av förordningens och direktivets krav.

Av förordningen och direktivet följer ett krav på att tillsynsmyndigheten ska vara inrättad med stöd av lag (artikel 54.1a i förordningen och artikel 44.1a i direktivet). Med detta ska, som redogjorts för i det föregående avsnittet, förstås både lag beslutad av riksdagen och förordning beslutad av regeringen. Att Datainspektionen är tillsynsmyndighet enligt det nuvarande dataskyddsdirektivet följer i dag av förordningen (2007:975) med myndighetsinstruktion, inte av lag. Vi anser att myndigheten även inom ramen för den nya ordningen kan inrättas genom bestämmelser i en förordning beslutad av regeringen.

9.3.3 Tillsynsmyndighetens organisation samt utnämning och avsättande av myndighetens ledamöter

Bedömning: Svensk rätt motsvarar i allt väsentligt dataskyddsförordningens och det nya dataskyddsdirektivets bestämmelser om tillsynsmyndighetens organisation och utnämningen respektive avsättandet av tillsynsmyndighetens chef. Detta gäller bland annat kraven på ett öppet rekryteringsförfarande, skydd mot godtyckligt avskedande och förbud mot förtroendeskadliga bisysslor, där allmänna författningsregleringar redan finns.

Förslag: Att chefen för Datainspektionen anställs genom beslut av regeringen för en period om minst fyra år, med möjlighet till förlängning, ska framgå av myndighetens instruktion.

Förordningen och direktivet

I dataskyddsförordningen och det nya dataskyddsdirektivet finns bestämmelser som bland annat rör utnämningen och avsättandet av ledamöter. Vidare finns vissa bestämmelser som kan sägas ta sikte på myndighetens organisation i övrigt. Några motsvarande bestämmelser finns inte i det nuvarande dataskyddsdirektivet.

Medlemsstaterna ska enligt dataskyddsförordningens artikel 53 föreskriva att varje ledamot av tillsynsmyndigheten ska utnämnas av parlamentet, regeringen, statschefen eller av ett särskilt oberoende, lagreglerat organ. Utnämningen ska göras genom ett öppet förfarande med insyn. I artikeln anges också att ledamöterna ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att de ska kunna utföra sitt uppdrag och utöva sina befogenheter. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med lagstiftningen i den berörda medlemsstaten. En ledamot får avsättas endast som en följd av grov försummelse eller när ledamoten inte längre uppfyller de villkor som krävs för att utföra uppdraget. Motsvarande bestämmelser finns i direktivet i artikel 43.

Av förordningen och direktivet följer vidare att medlemsstaterna ska säkerställa att varje tillsynsmyndighet väljer och förfogar över sin egen personal, som ska ta instruktioner uteslutande från tillsynsmyndighetens ledamöter (artikel 52.5 i förordningen och artikel 42.5 i direktivet).

Av artikel 54.1 i förordningen och artikel 44.1 i direktivet (tillsammans med beaktandesatserna 41 i förordningen och 33 i direktivet, se ovan) följer vidare ett krav på författningsreglering i medlemsstaterna för vissa regleringar som gäller utnämningen och avsättandet av tillsynsmyndighetens ledamöter. De kvalifikationer och de villkor för lämplighet som krävs för utnämning av ledamöter ska fastställas i författning, liksom regler och förfaranden för utnämningen. Ledamöternas mandattider och huruvida de ska kunna ges förnyat mandat ska också regleras, liksom villkor för utövande av tjänsten, förbud mot handlingar, yrkesverksamhet och förmåner och vilka bestämmelser som gäller för anställningens upphörande. Mandattiden för en ledamot får inte understiga fyra år, utom vid tillsättandet av de första ledamöterna efter det att förordningen har

trätt i kraft, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att garantera myndighetens oberoende (artikel 54.1 d) i förordningen och artikel 44.1 d) i direktivet).

Gällande svensk ordning för utnämning och avsättande av chefer för förvaltningsmyndigheter under regeringen samt övriga garantier för oberoende

Av 12 kap. 5 § regeringsformen följer att arbetstagare vid förvaltningsmyndigheter under regeringen anställs av regeringen eller av den myndighet som regeringen bestämmer. Vid beslut om sådana anställningar ska avseende fästas endast vid sakliga grunder, såsom förtjänst och skicklighet. Med förtjänst avses erfarenhet av tidigare tjänstgöring och med skicklighet lämplighet för den aktuella anställningen, genom utbildning, yrkeskunnande, prestationsförmåga osv. Skicklighet ska enligt 4 § lagen (1994:260) om offentlig anställning (LOA) sättas främst, om inte särskilda skäl talar för annat. Det grundlagsfästa kravet på sakliga grunder gäller alla anställningar, dvs. även av myndighetschefer.

Lagen (1982:80) om anställningsskydd, LAS, reglerar förhållandet mellan en arbetsgivare och en arbetstagare. Huvudregeln är att ett anställningsavtal gäller tills vidare (4 § LAS). I 1 § andra stycket LAS undantas vissa arbetstagargrupper från lagens tillämpning. Däribland finns arbetstagare ”som med hänsyn till arbetsuppgifter och anställningsvillkor får anses ha företagsledande eller därmed jämförlig ställning”. I förarbetena sägs att detta undantag gäller för bland annat generaldirektörer och överdirektörer vid statliga myndigheter, eftersom dessa arbetstagare har en utpräglad arbetsgivarfunktion och en särskild förtroendeställning i förhållande till arbetsgivaren.[9] I princip alla chefer för förvaltningsmyndigheter under regeringen har i dag tidsbegränsade förordnanden,[10] normalt för en period om sex år med en möjlig förlängning om högst tre år. Tiden som sådan är inte lagreglerad utan följer av förarbetsutta-

[9] Kungl. Maj:ts proposition nr 129 år 1973, prop. 1973:129 s. 194–195 och s. 230, prop. 1981/82:71 s. 92 f. och bet. InU 1973:36 s. 28.
[10] Det finns också ett fåtal myndighetschefer med fullmaktsanställningar.

landen och en sedan länge upparbetad praxis.[11] Kortare anställningstider än sex år förekommer i undantagsfall, t.ex. om det i förväg är känt att en myndighet ska omorganiseras eller om myndighetschefen kommer att uppnå pensionsåldern tidigare än inom sex år.

Ett tidsbegränsat förordnande kan inte sägas upp innan anställningstiden har löpt ut men myndighetschefen kan avskedas om han eller hon grovt har åsidosatt sina skyldigheter mot arbetsgivaren. Myndighetschefer med tidsbegränsade förordnanden kan vidare, av organisatoriska skäl eller annars av hänsyn till myndighetens bästa, förflyttas till en annan statlig anställning som tillsätts på samma sätt (32 § andra stycket och 33 § andra stycket LOA samt 18 § LAS).

Chefer för myndigheter under regeringen som har tidsbegränsade förordnanden kan under vissa förhållanden få inkomstgaranti och avgångsvederlag. Från och med den 1 januari 2017[12] gäller att den som är 61 år när en anställning upphör, då har haft en eller flera chefsanställningar under en sammanhängande period om minst sex år och som inte erbjudits en fortsatt anställning i samma befattning har rätt till inkomstgaranti. Garantin ska minskas med bland annat en annan pensionsgrundande inkomst. Oavsett chefens ålder kan avgångsvederlag betalas ut till den som haft en eller flera chefsanställningar oavbrutet i sex år. Också avgångsvederlagen ska minskas med andra inkomster.

Anställningar av myndighetschefer föregås numera i regel av ett öppet rekryteringsförfarande där den aktuella anställningen utannonseras. Inkomna ansökningshandlingar eller intresseanmälningar utgör allmänna handlingar när de har inkommit till Regeringskansliet. Sedan 2010 gäller enligt 39 kap. 5 b § offentlighets- och sekretesslagen (2009:400), förkortad OSL, att uppgifter om vem som sökt en anställning som chef för en förvaltningsmyndighet under regeringen kan omfattas av sekretess. Sekretessen gäller dock inte för beslutet i ärendet eller uppgiften om vem som har fått anställningen. Regeringen

[11] Vad gäller rektorer för universitet och högskolor finns det i förordning reglerat att dessa ska anställas för en tid om sex år. Anställningen kan förnyas högst två gånger om vardera tre år (2 kap. 8 § högskoleförordningen [1993:100]).

[12] Förordningen (2016:411) om tjänstepension, inkomstgaranti och avgångsvederlag till myndighetschefer ersätter den 1 januari 2017 förordningen (2003:55) om avgångsförmåner för vissa arbetstagare med statlig chefsanställning.

kan också enligt andra stycket meddela undantag från sekretessen. Denna möjlighet har i dag utnyttjats genom att det i 10 a § offentlighets- och sekretessförordningen (2009:641) anges att sekretess enligt 39 kap. 5 b § OSL inte gäller i ärenden om anställning av rektor vid ett universitet eller en högskola som har staten som huvudman och som omfattas av högskolelagen.

Sekretess hindrar heller aldrig att en uppgift lämnas till riksdagen (10 kap. 15 § OSL).

Regeringens utövande av sin utnämningsmakt anses vara en del av regeringens styrning av riket för vilken regeringen är ansvarig inför riksdagen (1 kap. 6 § regeringsformen).

Personalen vid en myndighet anställs av myndigheten.[13]

Att en förvaltningsmyndighet lyder under regeringen innebär, utöver att enskilda ministrar saknar befälsrätt över myndigheten, att föreskrifter och direktiv från regeringen ska riktas till myndigheten, inte till enskilda tjänstemän där.[14] Av LOA följer vidare ett förbud mot förtroendeskadliga bisysslor (7 §). Enligt bestämmelsen får en arbetstagare inte ha någon anställning eller något uppdrag eller utöva någon verksamhet som kan rubba förtroendet för dennes eller någon annan arbetstagares opartiskhet i arbetet eller som kan skada myndighetens anseende.

Datainspektionen är en s.k. enrådighetsmyndighet som leds av en myndighetschef (generaldirektör) som bistås av ett insynsråd. Insynsrådets uppgifter är att utöva insyn och att ge myndighetschefen råd. Insynsrådet har inga beslutsbefogenheter. Myndighetschefen är ordförande i insynsrådet och ska hålla rådet informerat om verksamheten.

Våra överväganden

Förordningen och direktivet talar om utnämnande och avsättande av tillsynsmyndigheternas ”ledamot eller ledamöter”. Detta tar enligt vår mening i ett svenskt perspektiv sikte på chefen för en förvaltningsmyndighet, i regel en generaldirektör. I en myndighet med ett kollektivt beslutsfattande torde dessutom ledamöterna i en styrelse eller nämnd omfattas av regleringen.

[13] 3 § anställningsförordningen (1994:373).
[14] Holmberg m.fl., Grundlagarna (3 uppl. 2012), s. 556.

Den svenska ordningen som har beskrivits ovan, som innebär delvis grundlagsfästa garantier för att endast sakliga skäl ska ligga till grund både för utnämning och avsättande av myndighetschefer, ett öppet rekryteringsförfarande samt lagreglerade förbud mot förtroendeskadliga bisysslor, uppfyller enligt vår mening förordningens och direktivets krav i dessa delar. Uppgifter om vilka som har sökt en utannonserad tjänst som chef för en förvaltningsmyndighet under regeringen kan visserligen omfattas av sekretess. Sekretessen tar sikte på allmänhetens möjligheter att med stöd av den svenska offentlighetsprincipen begära ut uppgifterna. Den hindrar däremot inte att utnämningsprocessen kan vara föremål för annan insyn, exempelvis inom ramen för riksdagens granskning av regeringen. Gör man en annan bedömning i denna del finns möjligheten för regeringen att föreskriva att sekretess inte ska gälla i ärenden om anställning av chef för Datainspektionen.

Det saknas enligt vår mening anledning att ändra på den ordning som innebär att Datainspektionen är en enrådighetsmyndighet som leds av en generaldirektör som utses av regeringen. Myndigheten anställer sin egen personal.

Förordningen och direktivet förutsätter också en nationell reglering av de kvalifikationer som krävs för en anställning som myndighetschef, förbud mot förtroendeskadliga bisysslor och villkor för anställningens upphörande.

Bestämmelser som förbjuder förtroendeskadliga bisysslor finns som nämnts i LOA. Vi menar vidare att det krav på förtjänst och skicklighet som följer av regeringsformen och LOA samt sakligheтskravet i 1 kap. 9 § regeringsformen sammantaget innebär ett krav på att den som anställs som chef för Datainspektionen ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området för dataskydd, som krävs för att ledamoten ska kunna fullgöra sitt uppdrag och utöva sina befogenheter.

Vad gäller föreskrifter om anställningens upphörande konstaterar vi att svensk rätt innehåller bestämmelser som ger ett starkt anställningsskydd och som innebär ett förbud mot godtyckliga avskedanden. En chef för en förvaltningsmyndighet under regeringen som har en tidsbegränsad anställning får visserligen förflyttas till en annan motsvarande statlig anställning. För detta förutsätts dock att en förflyttning krävs av organisatoriska skäl eller annars motiveras av hänsyn till myndighetens bästa. Även dessa

krav innebär enligt vår mening ett tillräckligt skydd mot att regeringen, som dessutom fattar sina beslut under parlamentariskt ansvar, på godtyckliga grunder gör sig av med en myndighetschef.

Om man vill förstärka detta skydd ytterligare skulle man kunna överväga att anställa chefen för Datainspektionen med fullmakt. De enda myndighetschefer som i dag är anställda med fullmakt är Justitiekanslern och Riksåklagaren. Att innehavare av dessa anställningar har ansetts böra ha ett ännu starkare anställningsskydd har förklarats med intresset av att rättskipningen är självständig och att dessa befattningshavares åtalsbedömningar står den dömande verksamheten nära.[15]

Om man vill ytterligare förstärka skyddet skulle man även kunna överväga att föreskriva ett undantag från förflyttningsmöjligheten för Datainspektionens chef, exempelvis genom följande tillägg (kursiverat) i 33 § andra stycket LOA:

> Är chefen för någon annan förvaltningsmyndighet som lyder omedelbart under regeringen anställd för bestämd tid, får han eller hon förflyttas till en annan statlig anställning som tillsätts på samma sätt, om det är påkallat av organisatoriska skäl eller annars är nödvändigt av hänsyn till myndighetens bästa. *Detta gäller dock inte chefen för Datainspektionen.*

Medlemsstaterna ska även genom en författningsreglering fastställa regler och förfaranden för att utse tillsynsmyndighetens ledamot eller ledamöter samt bestämmelser om ledamöternas mandattider. Den svenska ordningen, där myndighetschefer under regeringen utnämns av regeringen och förordnas för en tid om sex år, med en möjlig förlängning med ytterligare tre år, är inte författningsreglerad. Mot denna bakgrund föreslår vi en reglering i Datainspektionens myndighetsinstruktion där det fastställs att myndighetschefen anställs av regeringen för en period om minst fyra år, med möjlighet till förlängning. Förordningen föreskriver att den nationella regleringen också ska ange hur många gånger en anställning får förlängas. Vi menar att det med den föreslagna regleringen får anses framgå att regeringen är fri att förlänga anställningen hur många gånger som helst, vilket ur det oberoendeperspektiv som präglar förordningen torde vara acceptabelt.[16]

[15] Se t.ex. prop. 1975/76:105 bilaga 2, s. 210 och SOU 1992:60, s. 256 f.
[16] Om det bedöms lämpligare skulle ett alternativ kunna vara att införa en reglering motsvarande den som gäller för rektorer vid universitet och högskolor, se ovan.

9.3.4 Behöver tillsynsmyndigheten ytterligare befogenheter utöver dem som anges i dataskyddsförordningen?

Bedömning: Det saknas behov av att föreskriva att Datainspektionen ska ha ytterligare befogenheter utöver dem som följer av förordningen.

Bakgrund

Det ingår i vårt uppdrag att överväga om tillsynsmyndigheten bör ges andra befogenheter än de som anges i dataskyddsförordningen.[17] När det gäller anpassningar i svensk rätt med anledning av det nya dataskyddsdirektivet finns inte något motsvarande uttryckligt uppdrag till oss att överväga om tillsynsmyndighetens befogenheter.[18]

I artikel 58 i dataskyddsförordningen anges det vilka utredningsbefogenheter, korrigerande befogenheter samt befogenheter att utfärda tillstånd och att ge råd som de nationella tillsynsmyndigheterna ska ha. Här framgår att myndigheten som utredningsbefogenheter ska kunna

– beordra den personuppgiftsansvarige, personuppgiftsbiträdet eller deras företrädare att lämna all information som behövs för att myndigheten ska kunna fullgöra sina uppgifter,
– genomföra undersökningar i form av dataskyddstillsyn,
– genomföra en översyn av certifieringar som utfärdats i enlighet med artikel 42.7 i förordningen,
– meddela den personuppgiftsansvarige eller biträdet om en påstådd överträdelse av förordningen,
– från den personuppgiftsansvarige och ett biträde få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter, samt

[17] Dir. 2016:15 s. 10.
[18] Dir. 2016:21 s. 10–11.

– få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens eller medlemsstaternas processrätt.

En tillsynsmyndighet ska som korrigerande befogenhet enligt förordningen kunna

– utfärda varningar till en personuppgiftsansvarig eller till personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i förordningen,

– utfärda reprimander till en personuppgiftsansvarig eller biträdet om en behandling bryter mot förordningens bestämmelser,

– förelägga den personuppgiftsansvarige eller biträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt förordningen,

– förelägga en personuppgiftsansvarig eller ett biträde att se till att behandling sker i enlighet med förordningens bestämmelser och om så krävs på ett specifikt sätt och inom en specifik period,

– förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat,

– införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling,

– förelägga om rättelse eller radering av personuppgifter enligt artiklarna 16, 17 och 18 och lämna vissa underrättelser om detta,

– återkalla en certifiering eller beordra certifieringsorganet att inte utföra en certifiering,

– påföra administrativa sanktionsavgifter, samt

– förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

Slutligen ska en tillsynsmyndighet enligt förordningen ha sådana befogenheter att utfärda tillstånd och att ge råd som innebär att den kan

- ge råd till den personuppgiftsansvarige i enlighet med förordningens förfarande för förhandssamråd i artikel 36,
- på eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter,
- ge tillstånd till behandling enligt artikel 36.5 om medlemsstatens lagstiftning kräver ett sådant förhandstillstånd,
- avge ett yttrande om och godkänna utkast till uppförandekodexar enligt artikel 40.5,
- ackreditera certifieringsorgan enligt artikel 43,
- utfärda certifieringar och godkänna kriterier för certifiering enligt artikel 42.5,
- anta standardiserade dataskyddsbestämmelser enligt artiklarna 28.8 och 46.2 d,
- godkänna avtalsklausuler enligt artikel 46.3 a,
- godkänna administrativa överenskommelser enligt artikel 46.3 b, samt
- godkänna bindande företagbestämmelser enligt artikel 47.

Varje medlemsstat får enligt artikel 58.6 i lag ge sin tillsynsmyndighet ytterligare befogenheter, så länge sådana inte påverkar effektiviteten i samverkan mellan tillsynsmyndigheterna i de olika medlemsstaterna.

Det nuvarande dataskyddsdirektivets motsvarighet till uppräkningen av tillsynsmyndigheternas befogenheter är den mera begränsade regleringen i artikel 28, där det anges att en oberoende tillsynsmyndighet ska ha undersökningsbefogenheter, effektiva befogenheter att ingripa och befogenhet att inleda rättsliga förfaranden om överträdelser av direktivet eller att uppmärksamma de rättsliga myndigheterna på sådana överträdelser. De olika typerna av befogenheter exemplifieras i artikeln. Vissa av de krav som ställs

upp i det nuvarande direktivet regleras i dag i personuppgiftslagen. Det gäller bestämmelser om tillsynsmyndighetens tillgång till såväl personuppgifter och upplysningar som tillträde till lokaler (43 §), tillsynsmyndighetens möjligheter att under vissa förutsättningar döma ut vite (44–46 §§) samt rätten för tillsynsmyndigheten att efter bemyndigande från regeringen besluta om undantag från förbudet mot överföring av personuppgifter till tredje land. Resten har ansetts vara uppfyllda genom annan lagstiftning eller bedömts kunna genomföras i annan form än lag. Personuppgiftsförordningen och förordningen med instruktion för Datainspektionen är exempel på det sistnämnda.

Våra överväganden

Förordningens uppräkning av vilka befogenheter en tillsynsmyndighet ska ha är omfattande och såvitt vi kan bedöma tillräckliga för att myndigheten ska kunna fullgöra sina uppgifter. På grundval av det vi i dag känner till och kan överblicka saknas det därmed behov av att på nationell nivå föreskriva att Datainspektionen ska ha ytterligare befogenheter utöver dem som följer av förordningen.

9.3.5 Behövs det en kompletterande reglering av tillsynsmyndighetens uppgifter i myndighetsinstruktionen?

Bedömning: Det finns inget utrymme eller behov av en kompletterande reglering av Datainspektionens uppgifter i myndighetens instruktion.

Förslag: Datainspektionens instruktion ska inte längre ange att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud.

Tillsynsmyndighetens uppgifter enligt dataskyddsförordningen

I dataskyddsförordningens artikel 57 anges vilka uppgifter de nationella tillsynsmyndigheterna ska ha. I vårt uppdrag ingår att analysera vilket utrymme och behov det finns av regler om myndighetens uppgifter i instruktionen till myndigheten. Vi har inte fått motsvarande uppdrag när det gäller det nya dataskyddsdirektivet.

En tillsynsmyndighet ska enligt dataskyddsförordningen

- övervaka och verkställa tillämpningen av förordningen,
- öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn,
- i enlighet med nationell lagstiftning ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling,
- öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt förordningen,
- på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt förordningen, och om så krävs samarbeta med tillsynsmyndigheterna i andra medlemsstater för detta ändamål,
- behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet,[19]
- samarbeta, inbegripet utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att förordningen tillämpas och verkställs på ett enhetligt sätt,

[19] Av artikel 78.2 i förordningen följer att tillsynsmyndigheten inom tre månader ska informera den registrerade om hur handläggningen av ett klagomål fortskrider eller vilket beslut som har fattats med anledning av klagomålet.

– utföra undersökningar om tillämpningen av förordningen, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan myndighet,
– följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik och affärspraxis,
– anta sådana standardavtalsklausuler som avses i artiklarna 28.8 och 46.2 d,
– upprätta och föra en förteckning när det gäller kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4,
– ge råd om behandling av personuppgifter enligt artikel 36.2,
– främja framtagande av uppförandekoder enligt artikel 40.1 samt yttra sig över och godkänna sådana uppförandekoder som tillhandahåller tillräckliga garantier, i enlighet med artikel 40.5,
– uppmuntra till inrättandet av certifieringsmekanismer för dataskydd och av sigill och märkningar för dataskydd i enlighet med artikel 42.1 samt godkänna certifieringskriterierna i enlighet med artikel 42.5,
– i tillämpliga fall genomföra en periodisk översyn av certifieringar som utfärdats i enlighet med artikel 42.7,
– utarbeta och offentliggöra kriterier för ackreditering av ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43, samt ackreditera sådana organ,
– godkänna sådana avtalsklausuler och bestämmelser som avses i artikel 46.3,
– godkänna sådana bindande företagsbestämmelser som avses i artikel 47,
– bidra till dataskyddsstyrelsens verksamhet,
– hålla arkiv över överträdelser av förordningen och åtgärder som vidtagits i enlighet med artikel 58.2, samt
– utföra eventuella andra uppgifter som rör skyddet av personuppgifter.

Tillsynsmyndigheterna ska vidare underlätta inlämningen av klagomål, exempelvis genom framtagande av ett särskilt elektroniskt formulär. Utförandet av myndighetens uppgifter ska vara kostnadsfritt för den registrerade och för det eventuella dataskyddsombudet. Om en begäran är uppenbart ogrundad eller orimlig får dock tillsynsmyndigheten utkräva en rimlig avgift eller vägra att tillmötesgå begäran.

Dagens reglering i instruktionen för Datainspektionen

Av förordningen (2007:975) med instruktion för Datainspektionen följer att Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Myndigheten ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud. Myndigheten ska också följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.

Datainspektionen ska enligt sin instruktion också fullfölja förpliktelser och uppgifter som följer av vissa internationella dokument.

Våra överväganden

Dataskyddsförordningen är direkt tillämplig i medlemsstaterna och Datainspektionen ska därför direkt på grundval av förordningen ha de uppgifter som följer av denna reglering. Det saknas därför behov av att härutöver reglera dessa uppgifter i myndighetsinstruktionen. Vi ser heller inte något behov av att av andra skäl föreslå några kompletterande bestämmelser i instruktionen om Datainspektionens uppgifter. Härtill torde förordningens tydliga krav på tillsynsmyndigheternas oberoende göra att utrymmet för regeringen att styra Datainspektionen genom regleringar i myndighetsinstruktionen generellt är begränsat.

Kravet att tillsynsmyndigheterna ska vara oberoende gör vidare enligt vår mening att regeringens instruktion till Datainspektionen inte bör innehålla en bestämmelse med innebörden att vissa av de uppgifter som följer av dataskyddsförordningen pekas ut som mer angelägna än andra. Vi föreslår därför att den bestämmelse som säger att Datainspektionen särskilt ska inrikta sin verksamhet på att

informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen tas bort från myndighetsinstruktionen.

Våra överväganden om behovet av och utrymmet för att reglera Datainspektionens uppgifter gäller i förhållande till dataskyddsförordningen. I den utsträckning som Datainspektionen har uppgifter som faller utanför förordningens tillämpningsområde är regeringen fri att reglera myndighetens verksamhet.

9.3.6 Tillsynsmyndighetens resurser och anknytande frågor

Bedömning: Datainspektionen kommer att få nya och utvidgade uppgifter när de nya EU-rättsakterna ska tillämpas och vara implementerade i Sverige. Härutöver krävs redan dessförinnan ett omfattande förberedelsearbete. Detta förutsätter ökade resurser till Datainspektionen, främst i form av rekrytering av jurister och it-säkerhetspersonal.

Det går inte i dag mera exakt uppskatta storleken av resursbehovet. Ett säkrare underlag kan fås först när det genom det fortsatta arbetet med att anpassa svensk rätt och utformningen av tillsynen kan bedömas vad dataskyddsförordningen och det nya dataskyddsdirektivets kräver.

Förslag: De uppskattningar Datainspektionen hittills har gjort bör ligga till grund för det fortsatta arbetet med att bedöma myndighetens resursbehov.

Förordningen och direktivet

Av artikel 52.4 i förordningen och artikel 42.4 i direktivet följer att medlemsstaterna ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i dataskyddsstyrelsens verksamhet.

Datainspektionens bedömning av behovet av resurser

Datainspektionen har i budgetunderlaget för perioden 2017–2019 till regeringen anfört att få myndigheter har sett sitt arbetsområde förändras så radikalt som Datainspektionen gjort under de senaste 10–15 åren, med en kraftig ökning av digital behandling av personuppgifter inom både offentlig och privat verksamhet och en rasande snabb teknisk utveckling. Till detta kommer den kommande dataskyddsreformen inom EU, som enligt Datainspektionen innebär nya och förändrade uppgifter för myndigheten, men också ställer högre krav på myndigheter och företag som behandlar personuppgifter, vilket ökar behovet både av information och vägledning från Datainspektionen och av en effektiv tillsynsverksamhet.

Mot bakgrund av det omfattande arbete som krävs för att anpassa myndighetens organisation, arbetssätt, informationsmaterial m.m. efter förordningens och direktivets krav, men också för att i ett så tidigt skede som möjligt ge stöd och anvisningar till myndigheter och företag för att förbereda även dessa på reformen och därigenom öka förutsättningarna för ett gott integritetsskydd, anser Datainspektionen att myndighetens resurser behöver förstärkas med ytterligare anslagsmedel. Datainspektionens yrkande om resursförstärkning för budgetperioden 2017–2019 uppgår till 11 848 000 kronor för 2017, 16 677 000 kronor för 2018 och 16 677 000 kronor för 2019. Medlen ska enligt underlaget användas för att rekrytera ytterligare personal, i första hand jurister och it-säkerhetsspecialister. Datainspektionen räknar härutöver med ökade kostnader för bland annat lokaler, it-stöd och arbetsplatsutrustning.

Det som här redovisats om vad Datainspektionen anfört om resursbehovet är baserat på den bedömning Datainspektionen gjorde vid tidpunkten för budgetunderlaget. Arbetet med att bedöma behovet av resursförstärkningar med anledning av EU:s nya dataskyddsrättsakter fortsätter inom Datainspektionen.

Våra överväganden

De nationella tillsynsmyndigheterna får genom dataskyddsförordningen och det nya dataskyddsdirektivet omfattande och preciserade uppgifter inte minst när det gäller gränsöverskridande sam-

arbete och tillsynsåtgärder. Vi kan dessutom konstatera att dataskyddsförordningen är ett betydligt mer komplext regelverk än det nuvarande dataskyddsdirektivet och personuppgiftslagen och att det innehåller direktverkande EU-regler där förarbetsuttalanden och andra vägledande förarbeten saknas. Det nya dataskyddsdirektivet kommer också att innebära en detaljerad reglering av ett område som tidigare inte på EU-nivå har reglerats genom direktiv. Även inom EU, ibland annat i den nuvarande Artikel 29-gruppen där Datainspektionen medverkar, kommer det att krävas ett ökat förberedelsearbete för att omvandla gruppen till den dataskyddsstyrelse som föreskrivs av förordningen och direktivet. Detta arbete kommer att kräva ett omfattande förberedelsearbete även på hemmaplan.

Härutöver kan de nya rättsakterna förväntas medföra att klagomålshanteringen tar mer resurser i anspråk, som en följd både av tillsynsmyndigheternas skyldighet att behandla varje klagomål, de ökade mängder klagomål som kan förväntas bli en följd av e-tillgänglighetskravet och kravet att en klagande ska ha rätt att kräva biträde av Datainspektionen för kontakter med tillsynsmyndigheter i andra medlemsländer. Till detta kommer bestämmelser om bland annat gränsöverskridande personuppgiftsbehandling, godkännande av standardavtalsklausuler och förhandskontroller som också innebär ett ökat resursbehov för Datainspektionen.

Allt detta förutsätter, både före och efter rättsakternas ikraftträdande, att Datainspektionen tillförs resurser. Myndigheten behöver i första hand ytterligare personal, främst jurister och it-säkerhetspersonal. Det är för tidigt att mera exakt uppskatta storleken av resursbehovet. Det pågår ett arbete, både inom Datainspektionen och på annat håll, med att utreda och överväga vilka konsekvenser de nya rättsakterna får för hur tillsynen ska vara utformad i framtiden. Detta gäller inte minst de pågående utredningarna om anpassningar med anledning av dataskyddsförordningen och det nya dataskyddsdirektivet[20] som ska redovisa sina överväganden nästa år.

Mot bakgrund av de uppskattningar som i nuläget går att göra anser vi att Datainspektionens beräkningar bör ligga till grund för det fortsatta arbetet med att bedöma myndighetens resursbehov.

[20] Dir. 2016:15 och 2016:21.

I kapitel 11 återkommer vi till frågan om de ekonomiska konsekvenserna i övrigt av våra förslag om vissa förändringar av tillsynsansvaret.

10 Förstärkning av skyddet för den personliga integriteten genom vissa förändringar av tillsynsansvaret

10.1 Inledning

Vi har i kapitel 8 redovisat vår uppfattning att all tillsyn över behandling av personuppgifter varken kan eller bör samlas hos en enda myndighet. Dagens ordning bygger på att en central tillsynsmyndighet, Datainspektionen, har det centrala och mest omfattande tillsynsansvaret med ett mycket brett tillsynsområde. Att några myndigheter härutöver också har ett till vissa särskilda frågor begränsat tillsynsansvar är både nödvändigt och motiverat. Tillsynen skulle enligt vår uppfattning inte bli bättre eller effektivare, och skyddet för den personliga integriteten skulle därmed inte stärkas, om all tillsyn samlades hos en myndighet. Tvärtom skulle en sådan ordning innebära ett försämrat skydd för den enskildes integritet.

Vi har emellertid kunnat konstatera att det inom några områden finns förutsättningar att förbättra tillsynen ytterligare genom att på vissa punkter justera fördelningen av tillsynsansvaret och tydliggöra ansvarsfördelningen mellan olika myndigheter. Vi lämnar i det följande förslag på några sådana justeringar, som innebär en viss överföring av tillsynsansvar från andra myndigheter till Datainspektionen. Vår uppfattning är att dessa förslag stärker skyddet för den enskildes personliga integritet och bidrar till att tillsynsansvaret blir mer ändamålsenligt. Härtill kommer att dataskyddsreformen inom EU-rätten ställer vissa ytterligare krav på hur medlemsstaterna utformar sin tillsyn. Våra förslag är, så långt det i

nuläget är möjligt, anpassade efter dessa krav. Vi kan dock redan nu konstatera att de pågående utredningar som har i uppdrag att föreslå nödvändiga anpassningar av svensk rätt med anledning av EU:s dataskyddsreform[1] kan ha anledning att på nytt överväga vissa av de frågor som omfattas av vårt uppdrag.

10.2 Datainspektionens tillsynsansvar på området för elektronisk kommunikation

Förslag: Tillsynen över bestämmelserna i lagen om elektronisk kommunikation om abonnentförteckningar och s.k. cookies ska utföras av Datainspektionen i stället för av Post- och telestyrelsen. Kopplingen till sektorn elektronisk kommunikation är här svagare och prövningen tar sikte på mer allmänna dataskyddsrättsliga överväganden. Datainspektionen får härigenom ett mer samlat tillsynsansvar över behandling av personuppgifter.

Bedömning: För att utnyttja Datainspektionens expertkunskaper på området för integritetsskydd vid personuppgiftsbehandling och stärka Datainspektionens roll som central tillsynsmyndighet på området är det av värde om Post- och telestyrelsen samråder med Datainspektionen när frågor om innebörden av centrala dataskyddsrättsliga begrepp uppkommer i tillsynen. Det kan också bli aktuellt att hänskjuta frågor till Datainspektionen för avgörande. Möjligheterna till samråd och hänskjutande följer redan av lagstiftningen och kräver ingen ytterligare reglering. Även uppgifter som omfattas av sekretess torde kunna lämnas över.

[1] Främst Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiov (dir. 2016:15 och 2016:21).

10.2.1 Bestämmelserna om integritetsskydd i lagen om elektronisk kommunikation

Post- och telestyrelsen (PTS) är en av de myndigheter som vid sidan av Datainspektionen ska utöva tillsyn över behandling av personuppgifter. I förhållande till andra sådana myndigheter är PTS:s tillsynsområde på detta område relativt stort. PTS är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation (LEK), som i 6 kap. har bestämmelser om behandling av trafikuppgifter och integritetsskydd. Lagen, som till stor del bygger på det s.k. e-privacydirektivet,[2] är avsedd att skydda både den personliga integriteten och den mer omfattande rätten till förtrolig kommunikation. Rätten till förtrolig kommunikation innebär att såväl innehållet i en kommunikation som uppgifter som beskriver kommunikationen ska skyddas, oavsett om uppgifterna utgör personuppgifter eller inte.

Huvuddelen av bestämmelserna i 6 kap. LEK har ett nära samband med tillhandahållandet av elektroniska kommunikationstjänster eller elektroniska kommunikationsnät, och kan bara tillämpas mot den som tillhandahåller sådana tjänster och nät, s.k. operatörer. Bestämmelserna reglerar operatörernas hantering av uppgifter som förekommer just i samband med elektronisk kommunikation. Detta gäller t.ex. bestämmelser om behandling av trafikuppgifter, rätt för abonnenter att förhindra nummerpresentation och förbud mot avlyssning. Typiskt för dessa bestämmelser är därmed att de riktar sig främst mot operatörer och att de inte bara avser behandling av uppgifter som kan hänföras till en fysisk person (personuppgifter) utan också omfattar andra uppgifter som kommuniceras elektroniskt eller som beskriver kommunikationen. De uppgifter som omfattas av 6 kap. LEK är också sådana som typiskt sett är under överföring i ett elektroniskt kommunikationsnät, snarare än statiskt lagrade i t.ex. en databas. Uppgifterna är många gånger också ostrukturerade, till skillnad från uppgifter som återfinns i olika typer av register.

Som vi redan har konstaterat är det inte möjligt – och vore inte lämpligt, eftersom detta skulle förutsätta en granskning av inne-

[2] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

hållet i ett meddelande vilket i sig skulle vara tveksamt ur ett integritetsperspektiv – att för tillsynsändamål särskilja de meddelanden som innehåller personuppgifter från dem som inte gör det. Vidare är bestämmelserna om personlig integritet vid elektronisk kommunikation ofta systematiskt integrerade och starkt knutna till andra bestämmelser som reglerar sådan kommunikation. PTS är den myndighet som har den särskilda kompetensen på området för elektronisk kommunikation, och som är bäst lämpad att även inom ramen för tillsyn över integritetsskyddsbestämmelserna göra de överväganden som är specifika för detta område. Tillsynsansvaret för den absoluta huvuddelen av bestämmelserna i 6 kap. LEK ska därför ligga kvar hos PTS.

Vi har emellertid identifierat tre bestämmelser i LEK som avviker något från de övriga i 6 kap. och där det bör övervägas om tillsynsansvaret i stället bör ligga hos Datainspektionen. Det gemensamma för dessa bestämmelser är att kretsen av tillsynsobjekt typiskt sett är en annan, dvs. bestämmelserna riktar sig inte, eller endast till mycket liten del, till operatörer, och att kopplingen till den sektorsspecifika verksamheten inom elektronisk kommunikation är svagare.

Vi beskriver i de följande dessa bestämmelser och redovisar våra överväganden om tillsynsansvaret för dem. Vidare konstaterar vi att Datainspektionens roll som central tillsynsmyndighet med det övergripande ansvaret för tillsynen över behandling av personuppgifter skulle stärkas ytterligare om PTS under vissa förhållanden i ökad utsträckning samråder med Datainspektionen i frågor om personuppgiftsbehandling och i vissa fall till och med hänskjuter frågor till Datainspektionen för prövning.

Vid överväganden av dessa frågor bör den pågående översynen av e-privacydirektivet beaktas. EU-kommissionen antog den 6 maj 2015 sin strategi för en digital inre marknad[3] som bland annat syftar till att förbättra tillgången till digitala varor och tjänster för konsumenter och företag. I strategin ingår att genomföra en översyn av direktivet, enligt kommissionens meddelande för att stärka förtroendet och skärpa säkerheten för digitala tjänster och

[3] KOM (2015) 192 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska och sociala kommittén samt Regionkommittén ”En strategi för en inre digital marknad i Europa”.

hantering av personuppgifter. Kommissionens förslag till en ny reglering väntas i slutet av 2016. Det är inte möjligt att i nuläget bedöma omfattningen av översynen eller vilka bestämmelser som kan komma att omfattas av ett förslag till en ny reglering. Förändringarna kan komma att röra både det materiella innehållet i enskilda bestämmelser och mer övergripande frågor som vilka aktörer som ska omfattas av direktivet. Eftersom LEK till stora delar genomför direktivet, kan mer eller mindre omfattande förändringar av lagen behöva göras som ett resultat av översynen. Denna osäkerhet innebär att de förslag till författningsändringar som vi lägger fram kan komma att behöva revideras.

10.2.2 En överföring av visst tillsynsansvar till Datainspektionen

Bestämmelserna om abonnentförteckningar

Av 6 kap. 15 och 16 §§ LEK följer att en abonnent som är en fysisk person kostnadsfritt ska få information om ändamålen med en allmänt tillgänglig abonnentförteckning eller en förteckning ur vilken uppgifter kan erhållas genom abonnentupplysning, innan personuppgifter om abonnenten tas in i den. Om förteckningen ska finnas i elektronisk form ska abonnenten också informeras om de sökfunktioner som en sådan tjänst möjliggör. För att behandla personuppgifter om en abonnent som är en fysisk person i en abonnentförteckning krävs abonnentens samtycke. Abonnenten ska vidare ha möjlighet att utan kostnad kontrollera uppgifterna och få felaktiga uppgifter rättade samt att få uppgifter borttagna ur förteckningen så snart det är möjligt.

Bestämmelserna avser en verksamhet som numera bedrivs nästan uteslutande av företag som specialiserat sig på att sammanställa och förmedla bland annat person- och kreditinformation. Uppgifter om abonnenter, dvs. personer som har ingått avtal om elektroniska kommunikationstjänster, kan med stöd av 5 kap. 7 § första stycket 3 LEK inhämtas från operatörerna. Det förekommer i endast mycket begränsad omfattning att operatörerna själva bedriver abonnentupplysningsverksamhet.

Bestämmelserna i 6 kap. 15 och 16 §§ gäller endast abonnenter som är fysiska personer. Abonnentuppgifterna utgör därmed alltid

personuppgifter. Bestämmelserna gäller vidare endast förteckningar och är därmed inte, som många andra bestämmelser i LEK, tillämpliga på uppgifter under överföring eller uppgifter som t.ex. beskriver när var och med vem en abonnent har kommunicerat.

Den s.k. cookiebestämmelsen

Enligt 6 kap. 18 § LEK får uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Undantag görs för sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som abonnenten eller användaren uttryckligen har begärt.

Bestämmelsen reglerar s.k. cookies (kakor) och kallas därför ofta cookie-bestämmelsen. En cookie är en liten textfil som en webbplats kan begära att få spara i webbläsaren på besökarens dator. Textfilen används för att ge besökaren tillgång till olika funktioner på webbplatsen men också för att följa hur besökaren har använt webbplatsen, för att t.ex. anpassa de annonser som visas efter varje besökares intressen.

Bestämmelsen omfattar därmed alla som har en webbplats som använder cookies liksom alla som på något sätt lagrar eller hämtar redan lagrade uppgifter i en terminal, såsom en dator eller en mobiltelefon. Det rör sig därmed om en mycket vid krets tillsynsobjekt varav operatörer utgör endast en mycket liten del. Undantaget från informations- och samtyckeskravet för sådan lagring och åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät innebär dessutom att bestämmelsen i princip inte träffar den verksamhet som merparten av övriga bestämmelser i 6 kap. LEK avser att reglera, dvs. tillhandahållandet av elektronisk kommunikation och kommunikationsnät.

Den tillsyn som PTS har bedrivit mot innehavare av webbplatser har visat att den företeelse som bestämmelsen reglerar, själva överföringen av en cookie till eller från en besökares webbläsare, i många fall utgör endast en mindre del av en omfattande hantering

av uppgifter som syftar till att kartlägga besökarens personlighet eller intressen. Huvuddelen av en sådan kartläggning består i stället i den behandling av personuppgifter som utförs av t.ex. företag som förmedlar annonser till webbplatser, såsom samkörning av uppgifter om vilka webbplatser en besökare har varit inne på och vad han eller hon där har klickat på. Användningen av cookies är många gånger en förutsättning för att en sådan behandling ska kunna ske, men behandlingen utgör inte i sig den hantering av uppgifter som faller inom ramen för 6 kap. 18 § LEK. Denna bestämmelse reglerar med andra ord bara lagringen och inhämtandet av uppgifter, inte vad uppgifterna sedan används till. Därmed faller den efterföljande behandlingen utanför PTS:s tillsynsmandat och är i stället en fråga för Datainspektionens tillsyn.

Tillsyn över bestämmelserna om abonnentförteckningar och cookies bör utföras av Datainspektionen

De bestämmelser som har beskrivits här intar något av en särställning bland övriga bestämmelser i LEK som reglerar behandling av personuppgifter och integritetsskydd. De tar sikte på personuppgiftsbehandling som i huvudsak utförs av andra än operatörer, och de saknar även på andra sätt den nära koppling till sektorn elektronisk kommunikation som annars utmärker LEK. De avser i stället mer allmänna dataskyddsrättsliga förutsättningar för behandling av personuppgifter eller tar sikte på en mycket begränsad del av ett förlopp som i övrigt för närvarande regleras i personuppgiftslagen.

Bestämmelserna om abonnentförteckningar utgör, till skillnad från huvuddelen av den övriga regleringen i 6 kap. LEK, snarare en renodlad registerbestämmelse som, specifikt för behandling av personuppgifter i abonnentupplysningsändamål, gäller i stället för bland annat bestämmelsen i 10 § personuppgiftslagen om när behandling av personuppgifter är tillåten. Tillsynen över bestämmelserna förutsätter överväganden om bland annat krav på samtycke och information om ändamålen med en personuppgiftsbehandling. Denna typ av överväganden utgör en stor och självklar del av Datainspektionens tillsynsverksamhet. Tillsynen över bestämmelserna i 6 kap. 15 och 16 §§ LEK bör därför omfattas av Datainspektionens tillsynsmandat. Vi föreslår därför en sådan överföring av tillsynsansvar i denna del.

När det gäller den s.k. cookie-bestämmelsen finns dessutom en mycket nära koppling mellan själva användningen av cookies och den efterföljande behandlingen av de uppgifter som har samlats in med hjälp av cookies, men tillsynen utövas i dag av två olika myndigheter. Det är bara det första ledet i denna hantering – lagringen eller inhämtandet av uppgifter – som träffas av regleringen i 6 kap. 18 § LEK. Detta led utgör en mindre del av den omfattande hantering av uppgifter som syftar till att kartlägga besökarnas personligheter eller intressen. Resten av hanteringen utgörs av en behandling av de personuppgifter som har samlats in med hjälp av cookies och som i dag omfattas av Datainspektionens tillsyn. Tillsynen över användningen av cookies skulle enligt vår uppfattning bli mer effektiv och ändamålsenlig om en och samma myndighet kunde utöva tillsyn över hela det förlopp som börjar med användningen av cookies och övergår till en behandling av insamlade uppgifter. Vi föreslår därför att tillsynsansvaret också för bestämmelsen i 6 kap. 18 § LEK överförs till Datainspektionen.

Med de överföringar av tillsynsuppgifter till Datainspektionen som vi föreslår blir tillsynsansvaret mer ändamålsenligt fördelat. Det finns skäl att utgå ifrån att detta innebär ett stärkt skydd för den enskildes personliga integritet. Frågor som har en tydligare koppling till mer allmänna dataskyddsrättsliga principer samlas hos Datainspektionen som därigenom får en stärkt och tydliggjord roll som central tillsynsmyndighet med det övergripande ansvaret för tillsyn över personuppgiftsbehandling och som tillsynsmyndighet enligt den nya dataskyddsförordningen. Samtidigt skapas bättre förutsättningar för PTS att renodla sin tillsynsverksamhet till de bestämmelser som har den tydliga och nära kopplingen till sektorn elektronisk kommunikation. Vårt förslag föranleder ändringar i förordningen (2003:396) om elektronisk kommunikation och i Datainspektionens myndighetsinstruktion. Vi lämnar förslag på sådana ändringar.

De befogenheter som följer av LEK är inte identiska med de som gäller när tillsyn utövas med stöd av personuppgiftslagen. Det förefaller naturligt och vore också mest praktiskt att Datainspektionen vid tillsyn över de nämnda bestämmelserna i LEK kan ha tillgång till samma befogenheter som myndigheten har vid utövandet av annan tillsyn, dvs. de befogenheter som i dag följer av personuppgiftslagen. En sådan ordning skulle kunna åstadkommas

genom att i lagen eller förordningen om elektronisk kommunikation hänvisa till personuppgiftslagen. Mot bakgrund av det pågående arbetet med att anpassa svensk lagstiftning till den nya dataskyddsförordningen, vilket bland annat innebär att personuppgiftslagen inom kort kommer att upphävas, avstår vi emellertid från att nu lämna något sådant författningsförslag. I det lagstiftningsarbete som blir följden av den kommande översynen av e-privacydirektivet kan det också finnas anledning att återkomma till frågan om regleringen av tillsynsmyndigheternas befogenheter enligt LEK. Tills vidare anser vi att Datainspektionen, vid tillsyn av de bestämmelser i LEK som omfattas av våra förslag, ska ha samma befogenheter som PTS har i dag, det vill säga de som följer av LEK. Såvitt vi kan bedöma kommer detta inte att innebära några problem för tillsynsverksamheten.

10.2.3 En ytterligare förstärkning av Datainspektionens roll som central tillsynsmyndighet genom samråd och överlämnande av frågor för beslut

Också i sådana tillsynsärenden som med de förändringar vi nu föreslår även i fortsättningen ska omfattas av PTS:s tillsynsansvar uppkommer ibland frågor som kräver överväganden som har en direkt koppling till den generella personuppgiftsregleringen. Ett tydligt sådant exempel är om det i ett tillsynsärende uppkommer en fråga om innebörden av begreppet samtycke. Det handlar här om att prövningen i ett tillsynsärende förutsätter en tolkning av innebörden av ett begrepp som finns reglerat i LEK, och därför omfattas av PTS:s tillsynsansvar, men som också finns reglerat och har sin grund i personuppgiftslagen. För att ge ett så starkt skydd för den enskildes personliga integritet som möjligt är det centralt att sådana begrepp ges en både korrekt och enhetlig innebörd oavsett vilken myndighet som utövar tillsyn och oavsett vilken lag som tillämpas. Om det i ett tillsynsärende hos PTS uppkommer en fråga med sådan direkt koppling till innebörden av en generell personuppgiftsreglering, är det därför värdefullt om PTS inhämtar Datainspektionens vägledande yttrande i frågan. Det torde också i tillsynsärenden hos PTS kunna uppkomma situationer där det är lämpligare att en delfråga överlämnas till Datainspektionen för slutligt avgörande. Ett exempel kan vara om frågan om överföring

av personuppgifter till tredje land uppkommer i ett tillsynsärende. Prövningen gäller här tillämpningen av en bestämmelse i personuppgiftslagen som inte särskilt regleras i LEK.[4] Prövningen bör i sådana fall göras av Datainspektionen, varför det kan vara lämpligt att PTS överlämnar frågan dit för avgörande.

Ett utökat utnyttjande av möjligheten till samråd och överlämnande skulle ge Datainspektionen möjlighet att lämna stöd till PTS i tillsynsärenden där frågor uppkommer med en direkt koppling till den allmänna personuppgiftsregleringen. Härigenom stärks också Datainspektionens roll som central tillsynsmyndighet med det övergripande ansvaret för tillsyn över behandling av personuppgifter. För den enskilde skapas ett stärkt skydd för den personliga integriteten både genom att frågor om tolkningen av centrala dataskyddsregleringar avgörs med stöd av den myndighet som är expert på området och genom att det därigenom skapas ökade förutsättningar för enhetlighet i tillämpningen av aktuella bestämmelser.

Sådan samverkan mellan myndigheterna är redan i dag möjlig med stöd av förvaltningslagens (1986:223) bestämmelser och vi ser inte ett behov av ytterligare reglering.

Ett samråd med eller överlämnande av tillsynsärenden till Datainspektionen skulle kunna förutsätta att Datainspektionen får tillgång till uppgifter som hos PTS omfattas av sekretess. Det är inte ovanligt att det i PTS:s tillsynsärenden förekommer uppgifter som omfattas av sekretess enligt i 18 kap. 8 § och 30 kap. 23 § offentlighets- och sekretesslagen (2009:400), förkortad OSL. Av 18 kap. 8 § OSL följer att sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser bland annat telekommunikation eller system för automatiserad behandling av information. Sekretess gäller vidare enligt 30 kap. 23 § OSL i statlig tillsynsverksamhet bland annat för uppgifter om enskildas affärs- eller driftsförhållanden om det kan antas att det enskilde lider skada om uppgifterna röjs.

Sekretess gäller som huvudregel även mellan myndigheter. Den sekretessbrytande bestämmelsen i den s.k. generalklausulen i 10 kap. 27 § OSL torde emellertid enligt vår mening möjliggöra ett utbyte av uppgifter i de situationer av myndighetssamverkan som vi

[4] Jfr prop. 2010/11:46 s 58 ff.

har beskrivit. Ett informationsutbyte kan vara möjligt mellan myndigheter som har närbesläktade uppgifter och som båda har rättslig befogenhet att direkt fordra in uppgifterna i fråga. De nämnda primära sekretessbestämmelserna skulle vara tillämpliga även i Datainspektionen, varför uppgifterna även där skulle omfattas av sekretess.[5] Sekretess torde mot denna bakgrund inte utgöra något hinder mot den typ av ökad samverkan mellan PTS och Datainspektionen som vi föreslår.

10.3 Datainspektionens och Säkerhets- och integritetsskyddsnämndens parallella tillsynsuppdrag

Bedömning: Tillsynen över Säkerhetspolisens personuppgiftsbehandling bör utföras av både Datainspektionen och Säkerhets- och integritetsskyddsnämnden. Tillsynen över den öppna polisens personuppgiftsbehandling bör utföras av Datainspektionen.

Det nya dataskyddsdirektivet kommer att medföra vissa skyldigheter för tillsynsmyndigheten att på begäran av enskilda kontrollera lagenligheten av personuppgiftsbehandlingar även hos andra myndigheter än Polismyndigheten. Överväganden om den närmare utformningen av Datainspektionens skyldighet att på begäran av en enskild kontrollera om han eller hon har varit föremål för behandling av personuppgifter inom den öppna polisens brottsbekämpande verksamhet bör därför göras av den utredning som har i uppdrag att genomföra direktivet i svensk rätt.

Säkerhets- och integritetsskyddsnämndens anmälningsskyldighet till Datainspektionen bör gälla bara om det finns ett behov av ett rättsligt bindande och överklagbart beslut om exempelvis rättelse eller förbud mot fortsatt behandling. Detta bör anses vara fallet om Säkerhetspolisen inte vidtar nödvändiga åtgärder med anledning av nämndens uttalande om en otillåten personuppgiftsbehandling.

[5] Se också kommentaren till 10 kap. 27 § OSL i Offentlighets- och sekretesslagen, en kommentar, av Eva Lenberg m.fl.

Förslag: Tillsynen över den öppna polisens personuppgiftsbehandling bör inte längre ingå i Säkerhets- och integritetsskyddsnämndens uppdrag utan i fortsättningen endast utföras av Datainspektionen.

Säkerhets- och integritetsskyddsnämndens tillsynsuppdrag ska omfatta all behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet.

10.3.1 Parallella tillsynsuppdrag

Vår kartläggning har tydliggjort att den nuvarande ordningen, där både Datainspektionen och Säkerhets- och integritetsskyddsnämnden (SIN) har ett ansvar för tillsynen över polisens behandling av personuppgifter i den brottsbekämpande verksamheten, innebär att två myndigheter är behöriga men också faktiskt kommit att utöva tillsyn över samma personuppgiftsbehandling. I praktiken har den parallella tillsynen endast varit aktuell när det gäller Polismyndighetens (dvs. vad som ofta, och även i detta betänkande, kallas den öppna polisen, vilket därmed inte inkluderar Säkerhetspolisen) personuppgiftsbehandling[6] eftersom Datainspektionen hittills i princip inte har utövat någon inspektionsverksamhet som gäller Säkerhetspolisen.[7]

Att två myndigheter utövar tillsyn över samma verksamhet utan att det i det enskilda fallet är tydligt hur ansvaret för tillsynen ska fördelas kan innebära nackdelar. Vid sidan av de samhällsekonomiska invändningar som kan göras mot att ordningen innebär risker för dubbelarbete och ett ökat samordningsbehov, kan anföras att en oklar ansvarsfördelning är förvirrande både för den enskilde, som inte vet vart han eller hon ska vända sig, och för de berörda myndigheterna. När det gäller Datainspektionen och SIN har de två myndigheterna inte heller samma befogenheter: Datainspektionen kan till skillnad från SIN i rättsligt bindande beslut

[6] SIN:s tillsynsansvar omfattar även personuppgiftsbehandling enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister som utförs av Ekobrottsmyndigheten. Det är dock Polismyndigheten som är personuppgiftsansvarig för sådan behandling.

[7] Säkerhetspolisen samråder dock med Datainspektionen enligt 2 § polisdataförordningen (2010:1155) när myndigheten ska införa eller ändra i it-system av större omfattning eller med särskilda risker för intrång i den personliga integriteten.

förelägga en personuppgiftsansvarig att t.ex. rätta en felaktig uppgift eller upphöra med en felaktig behandling.

Å andra sidan var just den parallella tillsynen en omständighet som framhölls som en fördel när SIN fick sitt tillsynsuppdrag. Syftet var att därigenom skapa en stärkt och mera allsidig tillsyn, där två tillsynsmyndigheter med delvis olika fokus och uppdrag kunde komplettera varandra. SIN:s särskilda beslutsform, med en parlamentariskt förankrad nämnd, ansågs också vara en styrka och särskilt viktig för att tillgodose allmänhetens insyn. Man ville därigenom skapa förtroende för en verksamhet som innefattar särskilt integritetskänslig personuppgiftsbehandling och som omfattas av betydande sekretess. Till detta kom de krav på tillsynen som följde av en dom mot Sverige i Europadomstolen.[8]

Vi redovisar i det följande våra överväganden om för- och nackdelar med parallella tillsynsuppdrag när det gäller polisens personuppgiftsbehandling, liksom våra slutsatser i frågan om hur tillsynen bör vara utformad för att på bästa sätt bidra till ett starkt skydd för den enskildes integritet. Vi har funnit att en åtskillnad kan behöva göras mellan tillsynen över å ena sidan Säkerhetspolisens behandling av personuppgifter och å andra sidan den behandling som utförs av den öppna polisen.

10.3.2 Inrättandet av SIN och utvidgningen av myndighetens uppdrag

Bakgrunden till inrättandet av SIN var som nämnts att Europadomstolen hade funnit att Sverige saknade effektiva rättsmedel enligt artikel 13 i Europakonventionen. Talan hade väckts av ett antal personer som hade registrerats hos Säkerhetspolisen, men som helt saknade möjlighet att få ta del av de uppgifter som fanns registrerade.

Europadomstolen konstaterade att artikel 13 i Europakonventionen ställer upp ett krav på att enskilda ska ha tillgång till ett inhemskt rättsmedel för att kunna tillgodose sina rättigheter enligt konventionen. Rättsmedlet ska innebära att den behöriga nationella myndigheten både prövar ett klagomål i sak och har möjlighet att

[8] Dom i Europadomstolens mål Segerstedt-Wiberg m.fl. mot Sverige (ansökan nr 62332/00, dom den 6 juni 2006). Domen och dess konsekvenser beskrivs i nästa avsnitt.

besluta om lämplig gottgörelse. Rättsmedlet måste dessutom vara både praktiskt och rättsligt effektivt. Det krävs inte att varje enskilt rättsmedel anses effektivt, det kan räcka att de sammantaget uppfyller kraven på att erbjuda den enskilde ett effektivt rättsmedel. Domstolen noterade att både Justitieombudsmannen och Justitiekanslern är behöriga att ta emot och pröva klagomål från enskilda men att dessa myndigheter saknar befogenhet att fatta lagligt bindande beslut. Dessutom utövar de en allmän tillsyn och de har inget särskilt ansvar för att utreda hemlig övervakning eller lagring av uppgifter i Säkerhetspolisens register. Domstolen konstaterade vidare att den dåvarande Registernämnden inte hade någon befogenhet att besluta om att akter skulle förstöras eller uppgifter raderas alternativt rättas. Datainspektionen, som kan pröva klagomål från enskilda, har visserligen vidare befogenheter, men det hade enligt domstolen inte framkommit något som visade att Datainspektionen var effektiv i praktiken. De tillgängliga rättsmedlen kunde enligt domstolen därmed varken var för sig eller tillsammans uppfylla kraven enligt artikel 13.

Bland annat för att råda bot på denna brist inrättades SIN. Den nya myndighetens tillsynsområde omfattade ursprungligen brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter samt därmed sammanhängande verksamhet, liksom Säkerhetspolisens personuppgiftsbehandling. Nämnden skulle också på begäran av en enskild kontrollera bland annat om han eller hon varit föremål för sådan personuppgiftsbehandling i strid med lag eller annan författning. Syftet var att inrätta ett organ för löpande, rättslig kontroll av dessa verksamheter, som dessutom skulle stärka enskildas tillgång till ett nationellt effektivt rättsmedel. Nämndens parlamentariska anknytning, i form av ledamöter nominerade av riksdagens partigrupper, motiverades med att ett organ av detta särskilda slag bör vara utformat så att dess ledamöter kan sägas representera allmänheten och garantera medborgerlig insyn i verksamheten.[9]

I propositionen betonades att SIN inte ska överlappa utan komplettera andra tillsynsorgan och myndigheter. SIN gavs inte några befogenheter att på egen hand genom bindande beslut föreskriva t.ex. rättelse eller att en behandling ska upphöra. I stället

[9] Prop. 2006/07:133, s. 64 f.

anfördes att nämnden bör anmäla sina iakttagelser och överlämna relevanta delar av det som har framkommit i tillsyns- eller kontrollärendet till den myndighet som ansvarar för den fråga som är aktuell.[10] Anmälningsskyldigheten i förhållande till Åklagarmyndigheten, Justitiekanslern och Datainspektionen framgår i dag av 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

Vid införandet av den nya polisdatalagen (2010:361) utvidgades SIN:s tillsynsansvar till att även omfatta den öppna polisens personuppgiftsbehandling.[11] Alternativet att i stället anförtro tillsynen i dess helhet enbart åt Datainspektionen diskuterades i propositionen. Där anfördes att detta skulle innebära en begränsning vad gäller tillsynen över Säkerhetspolisens personuppgiftsbehandling. Det fanns enligt regeringen skäl som talade för att all tillsyn borde ligga på en enda myndighet men man ansåg att övervägande skäl talade för att tillsynen bäst utfördes av två olika myndigheter, var och en med utgångspunkt i sitt uppdrag. Därmed skulle SIN utöva en tillsyn som kompletterade Datainspektionens tillsyn. SIN hade enligt regeringen en sådan insikt i och erfarenhet av den granskade verksamheten som ökar förutsättningarna för en tillsyn som inriktas på de områden som kan ge upphov till särskilda risker från integritetssynpunkt. Datainspektionens tillsyn gav å sin sida goda förutsättningar att framför allt kontrollera att allmänna principer för behandling av personuppgifter tillämpas också inom den brottsbekämpande verksamheten. Det konstaterades vidare att en sådan ”dubbel” tillsyn redan förekom när det gällde Säkerhetspolisens personuppgiftsbehandling. Det anfördes i detta sammanhang inget om att SIN:s särskilda beslutsmodell och sammansättning med parlamentariskt deltagande skulle vara av särskilt värde när det gällde tillsynen över den öppna polisens personuppgiftsbehandling. Inte heller anfördes något om nödvändigheten av att på begäran av enskilda utföra kontroller av om de varit föremål för personuppgiftsbehandling av den öppna polisen.

[10] A. prop. s. 70.
[11] Prop. 2009/10:85, s. 273 f.

10.3.3 EU:s dataskyddsreform

Den nya allmänna dataskyddsförordningen och det nya dataskyddsdirektivet på det brottsbekämpande området antogs av rådet och parlamentet den 27 april 2016. Förordningen ska börja tillämpas den 25 maj 2018 och direktivet ska vara implementerat senast den 6 maj 2018. I kapitel 9 redovisar vi vårt förslag att Datainspektionen ska utses till nationell tillsynsmyndighet enligt de två rättsakterna.

Det nya dataskyddsdirektivet innehåller mera detaljerade bestämmelser om vilka krav som ställs på de nationella tillsynsmyndigheterna än det nuvarande rambeslutet. Den eller de myndigheter som ska vara ansvariga för att övervaka tillämpningen av direktivet ska vara oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter. En nationell tillsynsmyndighet måste vidare ha en mängd behörigheter, uppgifter och befogenheter som preciseras i direktivet. Här kan nämnas att tillsynsmyndigheten bland annat ska kunna utfärda varningar om att en planerad personuppgiftsbehandling sannolikt kommer att strida mot direktivet, förelägga om rättelse och förbjuda fortsatt behandling. Bindande beslut meddelade av en tillsynsmyndighet ska kunna överklagas för att garantera enskilda effektiva rättsmedel.

Den närmare innebörden av vissa av de krav som ställs upp i direktivet och vilka anpassningar som i några avseenden krävs när det gäller den svenska tillsynen har beskrivits i kapitel 9.

Att den öppna polisens personuppgiftsbehandling i brottsbekämpande verksamhet kommer att omfattas av direktivet är uppenbart. Frågan om och i vilken utsträckning direktivet kommer att omfatta också Säkerhetspolisens verksamhet är ännu svår att besvara. I direktiven till Utredningen om 2016 års dataskyddsdirektiv (dir. 2016:21) konstateras att centrala delar av Säkerhetspolisens verksamhet är av sådant slag att unionsrätten inte är tillämplig. Den utredningen har därför fått i uppdrag att bland annat analysera och bedöma på vilket sätt Säkerhetspolisens personuppgiftsbehandling bör regleras och om det finns skäl att separera den regleringen från polisdatalagstiftningen. Utredningens uppdrag ska redovisas senast den 30 september 2017. Vi utgår i våra överväganden ifrån antagandet att det nya dataskyddsdirektivet kan komma att anses tillämpligt på i vart fall delar av Säkerhetspolisens verksamhet. Utredningen om 2016 års dataskyddsdirektiv har även

i övrigt uppdrag som rör bland annat tillsynsmyndighetens uppgifter med anledning av direktivet. Denna del av uppdraget ska redovisas i ett delbetänkande senast den 1 april 2017.

10.3.4 Tillsynen över Säkerhetspolisens personuppgiftsbehandling bör utföras både av Datainspektionen och Säkerhets- och integritetsskyddsnämnden

När det gäller frågan hur tillsynen över Säkerhetspolisens personuppgiftsbehandling i fortsättningen bör vara utformad för att erbjuda ett så starkt och ändamålsenligt skydd som möjligt för den enskildes personliga integritet måste några särskilda omständigheter vägas mot de eventuella nackdelar som kan uppstå med en parallell tillsyn.

Europadomstolen fann i sitt nämnda avgörande att Datainspektionens tillsyn över Säkerhetspolisen, inte ens tillsammans med den tillsyn som också bedrivs av andra myndigheter, motsvarar Europakonventionens krav på ett effektivt rättsmedel. SIN tillkom bland annat för att råda bot på denna brist. Tillsynen över Säkerhetspolisens personuppgiftsbehandling kan mot den bakgrunden inte lyftas bort från SIN för att uteslutande utföras av Datainspektionen om inte sådana åtgärder vidtas som innebär att Datainspektionens tillsyn kommer att utgöra ett effektivt rättsmedel enligt artikel 13 i Europakonventionen. Exakt vilka åtgärder som detta skulle kräva är emellertid oklart.

Datainspektionen har inte SIN:s särskilda beslutsform, en nämnd med en parlamentarisk förankring. Denna beslutsform har ansetts särskilt lämplig i ärenden som präglas av så stark sekretess och begränsade möjligheter till insyn som Säkerhetspolisens säkerhets- och underrättelseverksamhet. Om Datainspektionen i fortsättningen ensam skulle ansvara för tillsynen över Säkerhetspolisens personuppgiftsbehandling måste det därför övervägas om en sådan särskild beslutsform bör införas även där.

Att tvärtom överväga en ordning som innebär att endast SIN i fortsättningen ska vara behörig att utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling skulle å andra sidan, i den mån det nya dataskyddsdirektivet kommer att anses omfatta i vart fall delar av Säkerhetspolisens verksamhet, förutsätta anpassningar till bland

annat direktivets krav på tillsynsmyndigheternas befogenheter. SIN saknar som angetts vissa av dessa befogenheter. SIN:s uttalanden är inte heller bindande beslut och de kan inte överklagas. Nämndens särskilda sammansättning med parlamentariskt utsedda ledamöter gör det enligt vår mening inte lämpligt att föreslå någon ändring i det avseendet.

I detta sammanhang kan vi också konstatera att Artikel 29-gruppen, dvs. den grupp inom EU med representanter för medlemsstaternas tillsynsmyndigheter som bland annat syftar till en enhetlig tillämpning av EU:s dataskyddsregler, har rekommenderat att tillsynen över säkerhets- och underrättelseverksamhet ska utföras av den nationella centrala tillsynsmyndigheten (i Sverige Datainspektionen) eller av ett särskilt organ i samarbete med den nationella tillsynsmyndigheten.[12] Dessa omständigheter talar mot att låta SIN ensamt ansvara för tillsynen över Säkerhetspolisen.

Sammantaget anser vi mot denna bakgrund att både Datainspektionen och SIN även i fortsättningen ska vara behöriga att utöva tillsyn över Säkerhetspolisens behandling av personuppgifter i den brottsbekämpande verksamheten. De två myndigheterna kan när det gäller Säkerhetspolisens personuppgiftsbehandling tillsammans tillhandahålla en ordning som ger ett starkt skydd för den enskildes personliga integritet. De parallella tillsynsbefogenheterna kompletterar här varandra och blir inte i praktiken behäftade med några sådana negativa konsekvenser som annars kan bli följden av en parallell tillsyn.

SIN har en väl upparbetad kunskap om och erfarenhet av de särskilda förhållanden som gäller för Säkerhetspolisens verksamhet, som ju omgärdas av stark sekretess och mycket begränsad insyn. Det finns vid SIN:s kansli och i nämnden en väl etablerad och fungerande ordning för att hantera det ofta omfattande hemliga material som utgör grunden för tillsynen. Nämndens särskilda sammansättning ger en stark parlamentarisk anknytning, med ledamöter som kan sägas representera allmänheten och garantera en medborgerlig insyn. Dessutom motsvarar den kontrollverksamhet som utförs av SIN, tillsammans med skyldigheten att anmäla förhållanden till myndigheter som kan fatta rättsligt bindande

[12] Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Article 29 Data Protection Working Party, 10 april 2014.

beslut, Europakonventionens krav på ett effektivt rättsmedel. Det kan tilläggas att det också i många andra länder är vanligt med särskilda tillsynsorgan för säkerhets- och underrättelseverksamhet.

För att leva upp till även de EU-rättsliga kraven på vilka befogenheter en tillsynsmyndighet bör ha, krav som kan komma att åtminstone till viss del omfatta även Säkerhetspolisens personuppgiftsbehandling, samt för att tillhandahålla en ordning som innebär att ett bindande beslut om exempelvis förbud eller rättelse kan meddelas och att ett sådant beslut också kan överklagas till allmän förvaltningsdomstol bör även Datainspektionen ha behörighet att med bibehållna befogenheter utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling. En sådan ordning är också lämplig med tanke på att Datainspektionen ska ha ett helhetsperspektiv när det gäller dataskyddsfrågor och följa utvecklingen på it-området. Detta gäller inte minst med tanke på det kommande arbetet inom dataskyddsstyrelsen.

En ordning som innebär att två myndigheter även i fortsättningen är behöriga att utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling stämmer dessutom väl överens med den som gäller på försvarsunderrättelseområdet. Statens inspektion för försvarsunderrättelseverksamheten (Siun) utövar sin tillsyn parallellt med Datainspektionen och denna ordning är av allt att döma inte ifrågasatt. De verksamheter som är föremål för tillsyn av SIN respektive Siun uppvisar likheter, särskilt vad gäller den starka begränsningen av allmänhetens insyn och behovet av särskilda tillsynsinsatser som kan stärka det medborgerliga förtroendet för verksamheterna.

I praktiken torde en ordning av detta slag innebära att de huvudsakliga tillsynsinsatserna på samma sätt som i dag kommer att utföras av SIN. I detta sammanhang bör SIN:s anmälningsskyldighet till Datainspektionen beröras. För att säkerställa en ordning som innebär att iakttagelser om otillåten personuppgiftsbehandling vid behov kan resultera i ett bindande och överklagbart beslut och som även tillgodoser de EU-rättsliga kraven på tillsynsmyndigheternas befogenheter, krav som till viss del kan komma att omfatta även Säkerhetspolisen, har vi övervägt om de finns behov av förändringar i den nuvarande ordningen beträffande när och hur SIN ska anmäla frågor om personuppgiftsbehandling till Datainspektionen. En sådan anmälningsskyldighet följer i dag av SIN:s

myndighetsinstruktion, som anger att SIN i ska anmäla vissa iakttagelser till Datainspektionen, Justitiekanslern och Åklagarmyndigheten.[13] Det är emellertid en skillnad mellan hur SIN:s anmälningsskyldighet är formulerad i förhållande till Datainspektionen respektive till de två andra myndigheterna.

SIN ska, om man i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, anmäla detta till Åklagarmyndigheten eller annan behörig myndighet. Om nämnden uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person ska nämnden anmäla detta till Justitiekanslern. Anmälningsskyldigheten i förhållande till Datainspektionen är däremot något svagare formulerad. Den förutsätter en mera fri bedömning av SIN om nämnden finner omständigheter som Datainspektionen bör uppmärksammas på, ska nämnden anmäla det till inspektionen. Våra kontakter med SIN och Datainspektionen har visat att myndigheterna har gjort något olika tolkningar av denna anmälningsskyldighet.

För att säkerställa att rättsligt bindande och överklagbara beslut ska kunna meddelas som föreskriver exempelvis att oriktigt behandlade personuppgifter ska rättas eller att en behandling ska upphöra, har vi övervägt att föreslå skärpningar av hur SIN:s anmälningsskyldighet till Datainspektionen formuleras. En sådan skärpning skulle kunna ske genom att SIN åläggs att göra en anmälan till Datainspektionen så snart nämnden har funnit förhållanden som utgör otillåten personuppgiftsbehandling. Vi har emellertid kunnat konstatera att även om SIN:s beslut inte är rättsligt bindande så följer polisen SIN:s uttalanden, något som enligt SIN är ett skäl till varför nämnden inte hittills haft anledning att göra någon anmälan till Datainspektionen. Till skillnad från vad som gäller i förhållande till Åklagarmyndigheten och Justitiekanslern – SIN kan inte själv fatta beslut om att inleda en förundersökning eller att tillerkänna någon skadestånd – har SIN därmed såvitt vi har kunnat finna i praktiken åstadkommit vad en anmälan till Datainspektionen skulle syfta till, dvs. exempelvis att en felaktig uppgift rättas eller att en otillåten behandling upphör. Det finns mot den bakgrunden inte skäl att nu införa en regel som kräver att SIN ska anmäla till Data-

[13] 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

inspektionen varje gång SIN konstaterat att det förekommit en otillåten personuppgiftsbehandling. En anmälningsskyldighet bör i stället föreligga bara när det finns ett behov av att Datainspektionen utnyttjar sina korrigerande befogenheter genom bindande och överklagbara beslut. Ett sådant behov uppkommer inte om Säkerhetspolisen självmant följer ett uttalande från SIN som pekar på ett behov av att vidta vissa åtgärder för att komma tillrätta med en felaktig behandling. Om det däremot skulle inträffa att Säkerhetspolisen inte rättar sig efter SIN:s uttalande i ett tillsynsärende, bör SIN anmäla detta till Datainspektionen, som då kan vidta åtgärder i form av exempelvis ett beslut med föreläggande om rättelse.

En sådan tolkning av innebörden av SIN:s anmälningsskyldighet i förhållande till Datainspektionen som den vi har beskrivit ryms enligt vår mening inom den nuvarande lydelsen av bestämmelsen. Det saknas därför behov av att genom författningsändringar skärpa anmälningsskyldigheten.

10.3.5 Tillsynen över den öppna polisens personuppgiftsbehandling bör utföras av Datainspektionen

När det så gäller den öppna polisens personuppgiftsbehandling i den brottsbekämpande verksamheten gör vi följande överväganden. De särskilda omständigheter som gäller beträffande tillsynen över Säkerhetspolisens personuppgiftsbehandling gör sig inte gällande med samma styrka när det gäller den öppna polisen. Det är inte här fråga om en verksamhet som i alla delar omgärdas av samma starka sekretess och begränsade insyn. När det gäller det från integritetssynpunkt allra känsligaste området, nämligen underrättelseverksamhet, kan dock sekretessen vara lika stark hos den öppna polisen som hos Säkerhetspolisen. Frågeställningen rör här främst, på ett nationellt plan, de principiella och samhällsekonomiska invändningarna mot parallell tillsyn samt de praktiska problem som riskerar att uppstå när det är oklart vilken myndighet som i ett enskilt fall ska inleda ett tillsynsärende.

När det gäller tillsynen över den öppna polisens personuppgiftsbehandling har tillsynsuppdraget i praktiken snarare kommit att vara parallellt än kompletterande. Ett exempel på detta för-

hållande är, som nämnts, tillsynsärendena om de s.k. kringresande- och kvinnoregistren som fördes av de dåvarande Polismyndigheterna i Skåne respektive Stockholm.[14] Det förstnämnda tillsynsärendet hanterades av SIN och det andra av Datainspektionen. I båda fallen var det fråga om personuppgiftsbehandling i den öppna polisens brottsbekämpande verksamhet och det kan för en utomstående vara svårt att förstå varför de inte prövades av samma myndighet. De frågeställningar som tillsynen avsåg var delvis likartade, vilket illustrerar risken för att de två myndigheterna skulle kunnat komma till oförenliga slutsatser. Som redan framhållits medför också de båda myndigheternas olika befogenheter och den omständigheten att Datainspektionens men inte SIN:s beslut kan överklagas, att det kan få betydelse vilken av myndigheterna som hanterar ett tillsynsärende.

Mot det nu sagda kan emellertid invändas att det var en förstärkning av tillsynen som man ville uppnå när SIN:s tillsynsuppdrag utvidgades till att också omfatta den öppna polisens personuppgiftsbehandling. Då anfördes som en fördel att de båda myndigheterna skulle utöva sin tillsyn med utgångspunkt i sina olika uppdrag. Datainspektionen skulle kontrollera att allmänna principer för behandling av personuppgifter tillämpades. Med tanke på att Datainspektionens tillsynsområde är så omfattande ansågs det vara av värde om inspektionens tillsyn kompletterades med tillsyn genom en myndighet som har till särskild uppgift att utöva tillsyn över brottsbekämpandeverksamhet. Tanken var att på detta sätt åstadkomma en mer allsidig och därigenom förstärkt tillsyn. Även om sekretessen i den öppna polisens brottsbekämpande verksamhet inte i alla delar är lika omfattande och stark som i Säkerhetspolisens underrättelseverksamhet är allmänhetens insyn även här i många fall begränsad. Att Datainspektionens tillsyn under sådana förhållanden kompletteras av ytterligare ett tillsynsorgan, som dessutom genom den parlamentariska anknytningen kan sägas representera allmänheten, bedömdes också vara en positiv förstärkning av tillsynen.

Ordningen med parallella tillsynsorgan har emellertid inte, på det sätt som avsågs, inneburit att de två myndigheterna utövar

[14] Säkerhets- och integritetsskyddsnämndens ärende med dnr 173-2013, uttalande den 15 november 2013 respektive Datainspektionens ärende med dnr 2790-2014, beslut den 24 juni 2015.

tillsyn med olika fokus. Datainspektionens och SIN:s tillsynsuppdrag kan avse samma frågeställningar, gälla samma regelverk och utövas med samma bedömningsgrunder. Tillsynen inriktas i båda fallen på de områden som kan ge upphov till särskilda risker från integritetssynpunkt. Intentionerna att Datainspektionen skulle kontrollera mer allmänna principer och att SIN skulle komplettera denna tillsyn med sin särskilda kompetens har därmed inte uppfyllts. Möjligen skulle fördelarna med den parallella tillsynen kunnat vara större om de två myndigheterna haft mer olika fokus, på det sätt som var förutsatt. Följden av att så inte blivit fallet är att två myndigheter med samma uppdrag utövar tillsyn över samma verksamhet, utan att de tänkta fördelarna med en granskning från olika utgångspunkter såvitt kan bedömas har uppkommit i praktiken.

Till detta kommer de praktiska invändningar som kan riktas mot den nuvarande ordningen. För att undvika kolliderande tillsynsinsatser för Datainspektionen och SIN en kontinuerlig dialog där de bland annat tar del av varandras tillsynsplaner. Genom löpande kontakter och utbyte av tillsynsplaner kan tillsynsinsatser som inriktas på samma frågor därigenom undvikas. Denna samordning tar emellertid i anspråk resurser utan att skapa något mervärde. Det finns även en risk att de två myndigheterna kan komma till olika slutsatser i fråga om en viss typ av behandling eller, som en följd av beslutens olika karaktär, att Datainspektionens beslut efter ett överklagande ändras medan SIN:s i princip likalydande uttalande i samma fråga fortfarande gäller och inte kan överklagas. I sådana situationer hjälper inte ett aldrig så väl utvecklat samråd mellan myndigheterna.

Ett så effektivt utnyttjande som möjligt av allmänna medel torde förutsätta att det inte finns några oklarheter i frågan om vilken myndighet som ska göra vad och att det inte finns risk för att två myndigheter gör samma sak. En ordning som innebär att det kan uppfattas vara en slump vilken av myndigheterna som inleder ett tillsynsärende är enligt vår mening inte lämplig.

Sammantaget anser vi därmed att den parallella tillsynen här, till skillnad från vad som gäller för tillsynen över Säkerhetspolisen, inte har fått de positiva effekter som eftersträvades. Den avsedda kompletteringen av Datainspektionens tillsyn har visserligen inneburit att fler tillsynsinsatser kunnat genomföras så att resultatet har blivit ”mer tillsyn”, men har samtidigt visat sig innebära praktiska

problem för både tillsynsobjekten och tillsynsmyndigheterna, oklarheter i ansvarsfördelningen och risker för ett ineffektivt utnyttjande av allmänna resurser. De avsedda förstärkningarna av skyddet för den enskildes personliga integritet har därför inte åstadkommits genom införandet av parallella tillsynsbefogenheter när det gäller den öppna polisens personuppgiftsbehandling.

Vi gör bedömningen att det inte är möjligt att genom lagstiftning eller på annat sätt formellt dela upp tillsynsansvaret på ett sådant sätt att de båda myndigheterna skulle kunna utöva tillsyn över den öppna polisen men inte ha ett överlappande tillsynsansvar. Det är svårt att se hur man på ett tillräckligt konkret och logiskt sätt skulle kunna definiera olika tillsynsuppgifter eller skiljelinjer mellan dem, och gränsdragningsproblemen skulle med en sådan lösning därmed sannolikt snarast förvärras.

Vi anser därför att övervägande skäl numera talar för att bara en myndighet ska utöva tillsyn över den öppna polisens personuppgiftsbehandling. I valet mellan Datainspektionen och SIN gör vi bedömningen att det bör vara Datainspektionen som har tillsynsansvaret för den öppna polisens personuppgiftsbehandling i den brottsbekämpande verksamheten. Det är bara Datainspektionen som i dag har de befogenheter som såvitt vi nu kan bedöma krävs av det nya dataskyddsdirektivet. Datainspektionen utövar vidare tillsyn över alla andra myndigheter i den så kallade rättskedjan; Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Kriminalvården. Datainspektionen deltar också i ett flertal gränsöverskridande samarbeten, såsom Europol, Schengens informationssystem och Prümrådsbeslutet. Utvecklingen både i Sverige och inom EU går mot ett ökat utbyte av personuppgifter mellan dessa myndigheter. För att säkerställa att tillsynen över flödet av personuppgifter ska bli effektiv och bedrivas med en helhetssyn är det en fördel om tillsynen över alla dessa myndigheters personuppgiftsbehandling utövas av en och samma myndighet. Datainspektionen har den breda erfarenhet och kompetens som krävs för att utöva en sådan samlad tillsyn.

Vi föreslår därför att SIN:s tillsynsuppdrag ändras så att det inte längre ska omfatta tillsyn över personuppgiftsbehandling i Polis-

myndighetens och Ekobrottsmyndighetens[15] brottsbekämpande verksamhet.

En ordning som innebär att endast Datainspektionen ska utöva tillsyn över personuppgiftsbehandlingen inom den öppna polisens brottsbekämpande verksamhet får till följd att Datainspektionen också bör ha en skyldighet att på begäran av en enskild kontrollera om han eller hon är föremål för en lagstridig personuppgiftsbehandling i den öppna polisens brottsbekämpande verksamhet. Med hänsyn till att det nya dataskyddsdirektivet ställer krav på tillsynsmyndigheten att utföra vissa kontroller på begäran av enskilda (artikel 46.1g) menar vi att den skyldighet som i dag åligger SIN inte bör överföras ordagrant till Datainspektionen. I stället bör den utredning som har i uppdrag att föreslå hur direktivet ska genomföras i svensk rätt, bland annat när det gäller tillsynsmyndighetens uppgifter, återkomma till frågan om hur Datainspektionens skyldighet att utföra kontroller på begäran av enskilda bör utformas.[16] En sådan skyldighet kommer dessutom så vitt vi kan bedöma att omfatta personuppgiftsbehandlingen i fler brottsbekämpande myndigheter än Polismyndigheten, såsom exempelvis Kustbevakningen och Tullverket.

Vi har ovan föreslagit att SIN även i fortsättningen ska utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling. Om tillsynen över den öppna polisens personuppgiftsbehandling bara ska utföras av Datainspektionen innebär detta att SIN:s verksamhet och uppdrag, såvitt gäller granskning av behandling av personuppgifter, återgår till den ordning som gällde före 2012. Utöver tillsynen över Säkerhetspolisens personuppgiftsbehandling kommer SIN även i fortsättningen att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter, och därmed sammanhängande verksamhet, samt på begäran av en enskild kontrollera om han eller hon i strid med lag har utsatts för hemliga tvångsmedel eller varit föremål för Säkerhetspolisens personuppgiftsbehandling. SIN kommer härutöver även i fortsättningen att bedriva den verksamhet som utförs av de två

[15] Det är Polismyndigheten som har personuppgiftsansvaret för behandling av personuppgifter enligt polisdatalagen vid Ekobrottsmyndigheten.
[16] Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06, dir. 2016:21).

särskilda organen Registerkontrolldelegationen och Skyddsregistreringsdelegationen.

10.3.6 SIN:s tillsynsuppdrag bör inte avgränsas till vissa lagar

SIN ska i dag enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet utöva tillsyn över den behandling av personuppgifter enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister som utförs av de myndigheter som omfattas av SIN:s tillsyn. När det gäller Säkerhetspolisen ska tillsynen också avse behandling enligt den gamla polisdatalagen (1998:622).

Att tillsynsuppdraget på detta sätt begränsas till två specifika lagar har visat sig leda till vissa tillämpningsproblem och osäkerhet om myndighetens tillsynsmandat i tillsynsärenden där en personuppgiftsbehandling även aktualiserar tillämpningen av någon annan registerlagstiftning. Osäkerheten förstärks när regeringen i förarbetena till annan lagstiftning anför att SIN:s tillsyn över personuppgiftsbehandling, trots den uttryckliga formuleringen i 1 § lagen om tillsyn över viss brottsbekämpande verksamhet, inte bara gäller polisdatalagen utan även närliggande lagstiftning.[17]

Vi menar att ett mera ändamålsenligt sätt att avgränsa SIN:s tillsynsansvar är att inte koppla det till personuppgiftsbehandling enligt vissa lagar. Uppdraget bör i stället formuleras så att SIN ska utöva tillsyn över den behandling av personuppgifter som utförs i brottsbekämpande verksamhet i de myndigheter som omfattas av tillsynen. Av våra tidigare förslag följer att detta kommer att innebära Säkerhetspolisen. Med en sådan avgränsning av tillsynsansvaret behövs inte heller någon särskild hänvisning till den gamla polisdatalagen.

[17] Se t.ex. prop. 2012/13:73, s. 114 f.

10.4 Frågan om ett integritetsskyddsråd

I vårt uppdrag har ingått att lämna förslag som innebär att den myndighet som ska ha det huvudsakliga ansvaret för tillsynen över behandling av personuppgifter är förberedd för att kunna fullgöra de uppgifter som Integritetskommittén (Ju 2014:09)kan komma att föreslå att ett integritetsskyddsråd ska ha.

Integritetskommittén redovisade den 7 juni 2016 i delbetänkandet Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén (SOU 2016:41) sina överväganden bland annat i frågan om ett integritetsskyddsråd (s. 646 f.). Kommittén anser att det inte bör inrättas något integritetsskyddsråd med huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen. Kommittén konstaterar att Datainspektionen redan i dag har ett övergripande ansvar för skyddet av personuppgifter, vilket bland annat innebär att myndigheten regelmässigt är remissinstans (både när det gäller formella remisser och delningar från departementen) och ofta finns representerad i utredningar som gäller sådana frågor. Det finns dessutom ett flertal andra myndigheter och organisationer, såsom Justitiekanslern, Riksdagens ombudsmän, Myndigheten för samhällsskydd och beredskap, PTS, SIN samt Advokatsamfundet, som också granskar förslag till ny lagstiftning ur ett integritetsskyddsperspektiv. Dessa bidrar enligt kommittén till att integritetsskyddsperspektivet lyfts fram i lagstiftningsarbetet och att bristfälliga avvägningar uppmärksammas.

Både riksdagen och regeringen har emellertid enligt kommittén behov av kunskap för att kunna följa den snabba utvecklingen på området, liksom kunskap om hur övervakning och kartläggning kan gå till och faktiskt förekommer. Kunskap behövs också om hur de legala förutsättningarna löpande förändras, vilka trender som kommer att vara av betydelse i framtiden och om hur stort det sammanlagda trycket blir på den enskilda individens privata sfär. Sådan kunskap behövs för att på olika sätt kunna påverka utvecklingen i önskvärd riktning, genom exempelvis ny lagstiftning, och för att bedöma effekterna av befintlig lagstiftning och andra åtgärder som innebär att enskilda registreras eller kartläggs. Också företag, myndigheter och enskilda personer kan enligt kommittén ha nytta av större kunskap och överblick.

Integritetskommittén konstaterar att det finns flera statliga myndigheter som arbetar med tillsyn av integritetsskydd men att tillsynen rör hur uppgifter hanteras i enskilda fall. Tillsynsverksamheterna innebär att tillsynsmyndigheterna får goda kunskaper om sina respektive ansvarsområden, men leder inte med nödvändighet till att tillsynsmyndigheterna kan skapa sig en övergripande och sammanlagd bild av hur omfattande kartläggningen och övervakningen av enskilda faktiskt är och hur den går till i praktiken. Det finns därmed enligt kommittén ett behov av att säkerställa att någon myndighet följer utvecklingen på ett mer övergripande plan och sammanfattar och analyserar nya trender, tekniker och användningsområden samt även hur de legala förutsättningarna löpande förändras.

Kommittén föreslår att detta behov av överblick ska tillgodoses genom att Datainspektionen regelbundet tar fram och offentliggör en sammanfattning och analys av den mest aktuella och betydelsefulla utvecklingen som påverkar den personliga integriteten. En sådan sammanställning och analys skulle t.ex. kunna innehålla redogörelser för ny teknik som ännu inte kommit till användning men är under utveckling, nya företeelser och tillämpningar i Sverige, intressanta händelser i andra länder, ny lagstiftning och förslag till lagstiftning, lagförslag som blivit liggande men som är önskvärda för att stärka integriteten samt även redogörelser för områden där det finns intressekonflikter mellan den operativa verksamheten och företrädare för integritetsintresset.

Det vore vidare enligt kommittén önskvärt med en analys av den sammantagna effekten som utvecklingen har eller kan få för enskildas personliga integritet och för samhällsutvecklingen i stort. Datainspektionen bör ges möjlighet att närmare bestämma rapportens innehåll; exempelvis är det troligen mer meningsfullt att koncentrera rapporten till några områden eller företeelser som förtjänar särskild uppmärksamhet, snarare än att eftersträva att den ska behandla all verksamhet i samhället där personuppgifter hanteras.

Arbetet med att ta fram rapporten skulle vidare ge Datainspektionen erfarenheter och kunskaper som kan komma till nytta i myndighetens tillsynsarbete. Datainspektionen skulle i arbetet med att ta fram rapporten också kunna dra nytta av sina redan etablerade kontakter med andra myndigheter som arbetar med omvärldsbevakning av integritetsskyddsfrågor, som exempelvis

Myndigheten för samhällsskydd och beredskap och PTS. Rapporten bör tas fram årligen och lämnas till regeringen, som i sin tur bör överlämna den till riksdagen i form av en årlig skrivelse som även innehåller regeringens egna kommentarer till rapporten. Med en sådan ordning skulle riksdagen få en samlad bild över vilka förslag som har lämnats och vilka åtgärder av betydelse för integritetsskyddet som har genomförts eller borde genomföras.

Integritetskommitténs ställningstagande i denna del innebär att det inte finns något behov för oss att lämna förslag som gäller ett integritetsskyddsråds uppgifter.

10.5 Vissa ytterligare myndigheters tillsyn

Bedömning: Fördelningen av tillsynsansvar mellan Datainspektionen och Centrala etikprövningsnämnden framgår redan av lagstiftningen och dess förarbeten och det saknas behov av ytterligare reglering. Datainspektionen ska således utöva tillsyn över om den personuppgiftsbehandling som utförs inom ramen för viss forskning är förenlig med personuppgiftslagen, medan Centrala etikprövningsnämnden utövar tillsyn över om forskning bedrivs i enlighet med etikprövningslagen. Det senare gäller även om forskningen innefattar behandling av personuppgifter.

Datainspektionen och Inspektionen för vård och omsorg har ett delvis överlappande tillsynsansvar, men myndigheterna har i grunden helt olika uppdrag. Det är centralt för skyddet av den personliga integriteten vid behandling av personuppgifter att sådana frågor prövas av Datainspektionen. Inspektionen för vård och omsorg bör därför samråda med Datainspektionen så snart det i inspektionens verksamhet uppkommer frågor om en viss personuppgiftsbehandlings lagenlighet. En sådan samrådsskyldighet är dock redan författningsreglerad.

Den rättsliga regleringen är i vissa fall utformad så att den ger sken av att några ytterligare myndigheter ska utöva tillsyn även över behandling av personuppgifter trots att detta sannolikt inte medvetet varit avsikten. Detta innebär emellertid enligt vad vi kunnat konstatera inga problem för tillsynen över behandling av personuppgifter eller för skyddet av den personliga integriteten,

eftersom tillsyn i praktiken ändå utförs av Datainspektionen även i dessa fall.

Det finns anledning att se över Datainspektionens tillsynsansvar enligt inkassolagen, i syfte att renodla och stärka Datainspektionens roll som central tillsynsmyndighet på området för integritetsskydd vid behandling av personuppgifter.

Ansvarsfördelningen mellan Centrala etikprövningsnämnden och Datainspektionen när forskning innefattar behandling av personuppgifter följer av den nuvarande lagstiftningen

Kartläggningen har visat att gränsdragningen mellan Datainspektionens och Centrala etikprövningsnämndens tillsyn i viss mån har uppfattats som oklar. Det är här inte fråga om parallella tillsynsuppdrag; lagstiftningen anger tvärtom tydligt att Centrala etikprövningsnämnden inte ska utöva tillsyn i den mån tillsynen faller inom någon annan tillsynsmyndighets ansvarsområde.[18] Förarbetena pekar här ut bland annat Datainspektionen.[19] Det råder däremot olika uppfattningar mellan Datainspektionen och Centrala etikprövningsnämnden om tolkningen av hur långt denna inskränkning i nämndens tillsynsmandat sträcker sig, där Centrala etikprövningsnämnden menar att den inte är behörig att utöva någon tillsyn alls så snart den forskning som nämnden har att pröva innefattar behandling av personuppgifter. Datainspektionen å sin sida menar att om prövningen förutsätter överväganden om forskningen i sig så åligger tillsynsansvaret Centrala etikprövningsnämnden. Detta gäller, enligt Datainspektionen, även om forskningen inbegriper behandling av personuppgifter.

Enligt vår uppfattning är den nuvarande lagstiftningen, med sina förarbeten, tydlig. Om personuppgifter behandlas inom forskning på ett sådant sätt att personuppgiftslagens bestämmelser blir tillämpliga kan och bör Datainspektionen utöva tillsyn över behandlingen. Är det exempelvis fråga om känsliga personuppgifter och behandlingen sker med stöd av 19 § personuppgiftslagen, kan Datainspektionen kontrollera om någon etikprövning har skett.

[18] 34 § lagen (2003:460) om etikprövning av forskning som avser människor.
[19] Prop. 2002/03:50 s. 163 f.

Detta är enligt bestämmelsen en förutsättning för att behandlingen ska få ske. Om etikprövning krävs men något etikgodkännande inte har lämnats av en etikprövningsnämnd, kan Datainspektionen förelägga den personuppgiftsansvariga att upphöra med behandlingen, eftersom den då strider mot personuppgiftslagen. Detsamma gäller om ett etikprövningsgodkännande har lämnats med villkoret att behandlingen förutsätter den enskildes samtycke men något samtycke inte har lämnats. Gemensamt för dessa frågeställningar är att syftet är att granska om den personuppgiftsbehandling som utförs inom ramen för forskningen är förenlig med personuppgiftslagen.

Är det i stället fråga om exempelvis att ta ställning till om forskningen i fråga behöver godkännas genom etikprövning eller om forskningen bedrivs i enlighet med ett gällande etikprövningsbeslut är Centrala etikprövningsnämnden, vars huvuduppgift är att utöva tillsyn över att forskning som avser människor bedrivs i enlighet med etikprövningslagen, den myndighet som är bäst lämpad att avgöra sådana frågor. Detta gäller även om den aktuella forskningen innefattar behandling av personuppgifter. En sådan ansvarsfördelning är också vad som beskrivs i förarbetena (prop. 2002/03:50, s. 164).

Att lagens och förarbetenas hänvisning till andra tillsynsmyndigheters ansvarsområde skulle innebära att Datainspektionen har att utöva tillsyn över alla frågor som rör forskning så snart denna innefattar behandling av personuppgifter, kan enligt vår mening inte ha varit avsikten. Datainspektionens uppdrag är att värna den personliga integriteten vid behandling av personuppgifter, medan Centrala etikprövningsnämndens uppdrag är att utöva tillsyn över efterlevnaden av etikprövningslagen och föreskrifter som har meddelats med stöd av den lagen. Skulle det däremot i ett tillsynsärende hos Centrala etikprövningsnämnden uppkomma frågor som avser huruvida behandlingen av personuppgifter har utförts i strid med personuppgiftslagen, bör denna fråga givetvis överlämnas till Datainspektionen.

Mot den redovisade bakgrunden finns det enligt vår uppfattning inget behov av författningsändringar som ytterligare reglerar ansvarsfördelningen mellan Datainspektionen och Centrala etikprövningsnämnden.

Inspektionen för vård och omsorg bör samråda med Datainspektionen i frågor som rör informationshantering inom vård och omsorg

När det gäller förhållandet mellan Datainspektionen och Inspektionen för vård och omsorg (IVO) och den tillsyn som de båda myndigheterna utövar över informationshanteringen inom vård och omsorg konstaterar vi att myndigheternas tillsynsansvar till viss del är överlappande. Samma informationshantering kan granskas av båda myndigheterna utifrån deras skilda uppdrag. Utan tillräcklig samordning riskerar detta att leda till oklarheter för de berörda verksamheterna och till att tillsynsmyndigheterna kan komma att lämna oförenliga besked. Vi har i samband med vårt kartläggningsarbete och i kontakter med myndigheterna särskilt noterat att de inte har en samstämmig bild av hur gränsdragningsproblemet ser ut, och att kommunikationen i frågan om vilken av myndigheterna som bör genomföra en tillsynsåtgärd inte alltid är tillräcklig.

Det är enligt vår mening inte möjligt att genom en rättslig reglering dela upp ansvaret mellan de båda myndigheterna så att risken för överlappningar försvinner. Frågor om integritet, patientsäkerhet, sekretess m.m. är i enskilda ärenden alltför sammanvävda med varandra för att en sådan uppdelning ska vara genomförbar, och en detaljerad reglering i lagstiftningen av vem som ska göra vad riskerar att ställa till fler problem än de löser.

De två myndigheterna har emellertid helt olika tillsynsuppdrag. Det är Datainspektionen som utövar tillsyn över att den personliga integriteten inte kränks vid behandling av personuppgifter. IVO:s uppdrag omfattar vård och omsorg och ett viktigt fokus ligger på patientsäkerheten. Det är därför nödvändigt och centralt för skyddet av den personliga integriteten att frågor om lagenligheten av personuppgiftsbehandling inte prövas av IVO utan av Datainspektionen.

IVO bör därför enligt vår mening i större utsträckning än vad som hittills skett samråda med Datainspektionen så snart det i tillsynsverksamheten uppkommer frågor om huruvida en viss behandling av personuppgifter är förenlig med personuppgiftslagen, patientdatalagen, lagen (2001:454) om behandling av personuppgifter inom socialtjänsten eller annan dataskyddslagstiftning. Detsamma gäller i arbetet med att ta fram riktlinjer som rör vård- och omsorgsgivares informationshantering. En sådan samverkansskyldighet följer redan i dag av 4 § i förordningen (2013:176) med

instruktion för IVO, där det slås fast att myndigheten ska samverka med andra berörda myndigheter i syfte att uppnå ett effektivt kunskaps- och erfarenhetsutbyte i arbetet med tillsyn, styrning med kunskap och regelgivning.

Det är viktigt att det inom IVO finns tillräcklig kunskap om de bestämmelser som gäller personuppgiftsbehandling eftersom den har stor betydelse för patientsäkerheten. Men det är samtidigt viktigt att man inom IVO accepterar och är medveten om att Datainspektionen är den myndighet som har bäst kunskap om och det övergripande ansvaret för behandling av personuppgifter också inom vård- och omsorg.

Till det som nu sagts ska läggas att EU:s dataskyddsförordning stärker betydelsen av den nationella tillsynsmyndigheten och dess roll som ytterst ansvarig för att dataskyddsförordningens bestämmelser tillämpas korrekt och enhetligt inom medlemsstaterna.

Att det finns ett behov av samråd visar också den omständigheten att berörda myndigheter före IVO:s tillkomst hade en särskild överenskommelse om hur ansvaret för tillsynen skulle fördelas. Vi menar att det kan finnas skäl att träffa en ny sådan överenskommelse och att det är viktigt att samrådsskyldigheten upprätthålls och utvecklas.

Regleringar som ser ut att ge ett tillsynsansvar över behandlingen av personuppgifter innebär inte ett problem i praktiken

Vi har i vårt kartläggningsarbete uppmärksammat vissa författningsregleringar som till synes ger vissa övriga myndigheter ett tillsynsansvar även över personuppgiftsbehandling men där sådan tillsyn inte utförs av myndigheterna. Det handlar här ofta om att en myndighet ska utöva tillsyn över efterlevnaden av en viss lag, exempelvis Naturvårdsverket över lagen (2004:1199) om utsläppsrätter, och att denna lag också innehåller några bestämmelser om behandling av personuppgifter. Det förekommer också regleringar som innebär att en myndighet pekas ut som både personuppgiftsansvarig och tillsynsmyndighet. Vår kartläggning visar att myndigheterna i fråga inte utför någon tillsyn över behandling av personuppgifter och många gånger inte ens är medvetna om att lagstiftningen kan sägas ge dem en sådan tillsynsuppgift. De uppger att de, om en fråga om personuppgiftsbehandling skulle aktualiseras vid

deras tillsyn, skulle överlämna frågan till Datainspektionen. Det har också visat sig att Datainspektionen ser sig oförhindrad att utöva tillsyn även i dessa fall, trots att lagstiftningen kan uppfattas ge en annan bild.

Även om avsikten sannolikt aldrig har varit att exempelvis Naturvårdsverket ska utöva tillsyn över personuppgiftsbehandling följer ett sådant tillsynsansvar uttryckligen av lagstiftningen. En rättslig reglering som oavsiktligt pekar ut en myndighet som tillsynsmyndighet är givetvis olycklig. I praktiken verkar regleringar av detta slag emellertid inte leda till gränsdragningsproblem eller oklarheter om vem som bör utöva tillsyn och de har därmed inte inneburit något problem för skyddet av den enskildes personliga integritet. Vi avstår därför från att nu föreslå någon ändring. Det kan finnas skäl att överväga om bestämmelserna i fråga bör bli föremål för översyn inom ramen för arbetet med de anpassningar som blir följden av EU:s dataskyddsreform.

Datainspektionens tillsyn enligt inkassolagen

Som framgår av vår kartläggning är Datainspektionen den tillsynsmyndighet som har det centrala och övergripande tillsynsansvaret på området för behandling av personuppgifter. Myndighetens huvudsakliga uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Datainspektionens roll och betydelse på området för dataskydd och personlig integritet kommer att öka när den nya dataskyddsförordningen ska börja tillämpas.

Datainspektionen ska i dag emellertid också utöva tillsyn enligt inkassolagen (1974:182). Inkassoföretag behandlar förvisso stora mängder uppgifter om gäldenärer och skulder. Många av dessa avser fysiska personer. Denna behandling av personuppgifter regleras av personuppgiftslagen och står under Datainspektionens tillsyn. Tillsynen enligt inkassolagen har emellertid sitt fokus på helt andra frågor än enskildas personliga integritet. Den syftar således främst till att undanröja risker för att en gäldenär utsätts för otillbörliga inkassoåtgärder och att garantera att inkassoföretag iakttar god sed i sin inkassoverksamhet. Datainspektionen tar dagligen emot klagomål från enskilda som anser att inkassoföretag

har handlat i strid med god inkassosed. Klagomålen gäller exempelvis att det har saknats grund för en fordran, att en fordran är preskriberad, att ett kravbrev har skickats till fel adress eller att inkassoföretaget har ansökt om ett betalningsföreläggande trots att fordran är bestridd i sak.

Datainspektionens tillsyn över efterlevnaden av inkassolagen avviker således i hög grad från syftet med myndighetens övriga tillsynsverksamhet, att skydda människor mot intrång i den personliga integriteten vid behandling av personuppgifter. Genom att skapa förutsättningar för Datainspektionen att i ännu högre grad använda sina resurser på tillsyn över behandling av personuppgifter skulle dess uppgift som central tillsynsmyndighet renodlas och stärkas. En sådan renodling ligger också i linje med den förändring av Datainspektionens verksamhet som EU:s dataskyddsreform kommer att medföra.

Den nu gällande ordningen innebär dessutom att det finns en uppdelning av tillsynsansvaret över inkassoföretag mellan Datainspektionen och Finansinspektionen. Allt fler inkassoföretag ägnar sig numera också åt sådan verksamhet som står under Finansinspektionens tillsyn, såsom kreditgivning. I sådana fall ska tillsynen bara utövas av Finansinspektionen, dvs. även när det gäller sådana frågor om god inkassosed som annars hade stått under Datainspektionens tillsyn. Gränsdragningen mellan de två myndigheternas tillsynsbefogenheter kan medföra praktiska och principiella problem. Det kan vara svårt för gäldenärer att veta till vilken av myndigheterna man ska vända sig för att påtala brister i en inkassoverksamhet och de parallella tillsynsuppdragen kan medföra risker för olika bedömningar och praxis på inkassoområdet. Detta kan leda till att tillsynen blir både ineffektiv och oförutsägbar.

Mot denna bakgrund anser vi att frågan om att föra över Datainspektionens tillsynsansvar enligt inkassolagen till någon annan myndighet, närmast Finansinspektionen, bör utredas. Frågan ligger dock utanför vårt egentliga utredningsuppdrag varför vi inte utvecklar den ytterligare här.

11 Konsekvenser av utredningens förslag m.m.

11.1 Inledning

En utredning ska enligt kommittéförordningen (1998:1474) redovisa vilka konsekvenser förslagen i ett betänkande kan få i olika avseenden. I förordningens 14 § föreskrivs att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt så ska dessa redovisas. Enligt 15 § i förordningen ska vidare redovisas eventuella konsekvenser för den kommunala självstyrelsen. Detsamma gäller eventuella konsekvenser för brottsligheten och det brottsförebyggande arbetet, samt för bland annat sysselsättning och offentlig service i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag samt för jämställdheten mellan kvinnor och män.

11.2 Konsekvenser av våra förslag

Det pågår ett omfattande arbete inom Regeringskansliet, bland annat i form av ett stort antal utredningar, som på olika sätt berör den personliga integriteten och tillsyn över behandlingen av personuppgifter. Flera av dessa kan komma att påverka både hur den centrala tillsynsmyndigheten, Datainspektionen, andra myndigheter med tillsynsuppgifter men också ytterligare myndigheter behöver arbeta och vara organiserade. Detta gäller i hög grad för de utredningar som har i uppdrag att analysera vilka anpassningar som är nödvändiga med anledning av EU:s nya dataskyddsförordning och

dataskyddsdirektiv. Det kan redan nu konstateras att rättsakterna i sig innehåller omfattande bestämmelser om de nationella tillsynsmyndigheternas uppgifter, befogenheter och inbördes samverkan, som såvitt vi nu kan bedöma kommer att innebära utökade uppgifter för främst Datainspektionen.

Dessa omständigheter innebär att det är svårt att i nuläget bedöma vilka ekonomiska konsekvenser våra förslag skulle få. Genomförandet av dem och de förslag som kan bli resultatet av övriga utredningar måste också rimligen ske samordnat. Våra bedömningar när det gäller konsekvenserna av våra förslag kan därför inte bli annat än preliminära uppskattningar.

Vi har bett Datainspektionen, Säkerhets- och integritetsskyddsnämnden (SIN) samt Post- och telestyrelsen (PTS) att göra uppskattningar av vilka konsekvenser våra förslag skulle få. Av det underlag vi har fått drar vi följande slutsatser.

När det gäller förslaget att endast Datainspektionen ska utöva tillsyn över personuppgiftsbehandling i den öppna polisens brottsbekämpande verksamhet har Datainspektionens gjort bedömningen att myndigheten för att ensam utföra det här tillsynsuppdraget behöver tillföras resurser som motsvarar fyra helårsarbetskrafter, till en uppskattad kostnad av drygt 4 miljoner kronor per år. SIN bedömer att tre årsarbetskrafter i dag ägnar sig åt den öppna polisens personuppgiftsbehandling. Kostnaderna för kontrollärenden som avser den öppna polisens personuppgiftsbehandling utgör enligt SIN ungefär hälften av de totala kostnaderna för tillsynen på detta område.

Mot bakgrund av de redovisade uppgifterna bedömer vi att våra förslag i denna del kommer att innebära ett behov av personalförstärkningar för Datainspektionen som motsvarar fyra helårsarbetskrafter. När det gäller konsekvenserna för SIN om tillsynsuppdraget minskar i motsvarande mån kan man givetvis hävda att resultatet av våra förslag bör vara kostnadsneutralt. Vi menar dock att den överflyttning av uppgifter som vi föreslår inte bör föranleda minskade anslag för SIN. Uppdraget att utöva tillsyn över Säkerhetspolisen är särskilt viktigt och centralt för att värna enskildas integritet. Tillsynen avser här en verksamhet där den enskilde till stor del helt saknar möjlighet till insyn och där brister kan få allvarliga konsekvenser för den drabbade. SIN:s tillsynsuppdrag är inte bestämt definierat utan myndigheten avgör själv

hur tillgängliga resurser ska fördelas på olika tillsynsinsatser. Med den överflyttning av tillsynsansvar som vi föreslår finns förutsättningar för SIN att koncentrera och utöka sin tillsyn när det gäller den för enskilda särskilt integritetskänsliga personuppgiftsbehandling som utförs av Säkerhetspolisen. Med tillräckliga resurser för en sådan tillsyn stärks skyddet för den enskildes personliga integritet.

Förslaget att överföra tillsynsansvaret för bestämmelserna om abonnentförteckningar och s.k. cookies från PTS till Datainspektionen bedöms få begränsade effekter. Sammantaget gör vi bedömningen att Datainspektionen här kan behöva en resursförstärkning motsvarande en och en halv helårsarbetskraft, till en uppskattad kostnad av ungefär 1,5 miljoner kronor per år. Det ökade resursbehovet avser främst tillsynen över den s.k. cookiebestämmelsen, som har sin grund i EU:s e-privacydirektiv och som ofta är föremål för diskussion och ökad uppmärksamhet på EU-nivå. För PTS blir effekterna av överföringen av tillsynsansvar såvitt vi kan bedöma marginella. Detta förklaras av att de faktiska tillsynsinsatser som gällt de aktuella bestämmelserna, som en följd av de begränsningar som ligger i att bestämmelserna saknar en koppling till myndighetens övriga verksamhet, har varit mycket begränsade.

Vi har ovan betonat att Inspektionen för vård och omsorg (IVO) i högre utsträckning än vad som hittills skett bör samråda med Datainspektionen när det i dess tillsynsveksamhet uppkommer frågor om huruvida en viss behandling av personuppgifter är förenlig med dataskyddslagstiftningen. Vilka ekonomiska konsekvenser ett sådant ökat samråd skulle få för Datainspektionen är svåra att uppskatta. Behovet av resurser beror på hur många ärenden IVO i praktiken väljer att samråda om. Det bör dock noteras att IVO är en stor myndighet med ett omfattande tillsynsverksamhet. Även om IVO samråder med Datainspektionen i endast en mindre del av alla tillsynsärenden skulle det kunna innebära en påtaglig ökning av Datainspektionens arbete. En preliminär uppskattning innebär att Datainspektionen i denna del behöver förstärkas med fyra helårsarbetskrafter, till en kostnad av drygt fyra miljoner kronor. Även för IVO kan ett ökat utnyttjande av samrådsmöjligheten få konsekvenser för arbetssätt och organisation. Dessa är dock svåra att

bedöma och det kan där i stället för ökade kostnader medföra effektivitetsvinster.

Med de personalförstärkningar vi preliminärt bedömer att Datainspektionen har behov av med anledning av våra förslag, och med de förstärkningar som kan bli resultatet av de övriga utredningar som rör Datainspektionens uppdrag och arbetssätt, bedömer myndigheten att det kan bli nödvändigt att byta lokaler. Man anser dock att det är för tidigt för att nu kunna göra några bedömningar i den delen.

Vi ser inte att våra förslag kommer att innebära några konsekvenser för den kommunala självstyrelsen, brottsligheten och det brottsförebyggande arbetet, eller för någon av de andra uppräknande aspekterna, såsom sysselsättning och offentlig service i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag eller för jämställdheten mellan kvinnor och män.

Vi har också i kapitel 9 redovisat våra överväganden i frågan om Datainspektionens resursbehov med anledning av EU:s dataskyddsreform.

11.3 Ikraftträdande- och övergångsbestämmelser

Den nyligen beslutade reformen på EU:s dataskyddsområde, med en ny allmän dataskyddsförordning och ett nytt dataskyddsdirektiv på det brottsbekämpande området, innebär att det i ett stort antal utredningar pågår ett omfattande arbete med att anpassa svensk rätt till de nya rättsakterna. Detta arbete kan komma att få betydelse för hur Datainspektionen och andra tillsynsmyndigheter arbetar. Hur den slutliga författningsregleringen av tillsynsmyndigheternas verksamhet bör utformas med anledning av dataskyddsreformen måste, för att få till stånd en fungerande och konsistent reglering, övervägas i ett sammanhang. Det kan då också finnas anledning att överväga behovet av övergångsbestämmelser.

Mot denna bakgrund avstår vi från att nu ange något bestämt ikraftträdandedatum för våra föreslagna författningsförändringar. En rimlig utgångspunkt är dock att de bör träda i kraft senast i maj 2018.

12 Författningskommentar

12.1 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

1 §

Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

Nämnden ska även utöva tillsyn över *behandlingen* av personuppgifter *i Säkerhetspolisens brottsbekämpande verksamhet.* Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § polisdatalagen (2010:361).

I paragrafen beskrivs Säkerhets- och integritetsskyddsnämndens tillsynsområde. Förslaget innebär dels att tillsynen bara ska omfatta sådan behandling av personuppgifter i brottsbekämpande verksamhet som utförs av Säkerhetspolisen, dels att tillsynen ska omfatta all personuppgiftsbehandling i denna verksamhet, och inte endast sådan behandling som följer av vissa, gällande eller upphävda, lagar. Ändringen behandlas i avsnitt 10.3.4.

12.2 Förslaget om förordning med ändring i förordningen (2003:396) om elektronisk kommunikation

2 §

Post- och telestyrelsen är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation. *Datainspektionen är dock tillsynsmyndighet såvitt avser 6 kap. 15, 16 och 18 §§ i den lagen.*

Post- och telestyrelsen ska för Sveriges del fullgöra de uppgifter som den nationella tillsynmyndigheten har enligt

1. Europaparlamentets och rådets förordning (EU) nr 531/2012 av den 13 juni 2012 om roaming i allmänna mobilnät i unionen, och
2. Europaparlamentets och rådets förordning (EU) nr 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster och förordning (EU) nr 531/2012 om roaming i allmänna mobilnät i unionen.

Paragrafen innebär en precisering av vilken myndighet som är tillsynsmyndighet enligt lagen (2007:389) om elektronisk kommunikation. Ändringen innebär att tillsyn över efterlevnaden av bestämmelserna om abonnentförteckningar och s.k. cookies ska utövas av Datainspektionen i stället för av Post- och telestyrelsen. Ändringen behandlas i avsnitt 10.2.2.

12.3 Förslaget till förordning med ändring i förordningen (2007:975) med instruktion för Datainspektionen

1 §

Datainspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet.

Myndigheten ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.

I paragrafen anges Datainspektionens övergripande uppgifter. Ändringen innebär att det inte längre föreskrivs att myndigheten särskilt ska inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen. Ändringen behandlas i avsnitt 9.3.5.

2 a §

Myndigheten är tillstånds- och tillsynsmyndighet enligt kreditupplysningslagen (1973:1173) och inkassolagen (1974:182).

Myndigheten är tillsynsmyndighet enligt

– *artikel 51.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), och*

– *artikel 41.1 i Europarlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.*

Myndigheten ska delta i den europeiska dataskyddsstyrelsens arbete.

Myndigheten är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation såvitt avser 6 kap. 15, 16 och 18 §§ i den lagen.

Paragrafen anger enligt vilka lagar och EU-rättsakter Datainspektionen är tillsynsmyndighet. Ändringen i *andra stycket* innebär att Datainspektionen är tillsynsmyndighet enligt den allmänna dataskyddsförordningen och det nya dataskyddsdirektivet på det brottsbekämpande området. Ändringen behandlas i avsnitt 9.3.2.

Ändringen i *tredje stycket* behandlas i avsnitt 9.3.2 och innebär att Datainspektionen ska delta i den europeiska dataskyddsstyrelsens (European Data Protections Board, EDPB) arbete.

Ändringen i *fjärde stycket* innebär ett tydliggörande av att tillsyn över bestämmelserna om abonnentförteckningar och s.k. cookies ska utföras av Datainspektionen i stället för av Post- och telestyrelsen. Ändringen behandlas i avsnitt 10.2.2.

4 §

Myndigheten är nationell tillsynsmyndighet enligt

– artikel 114 i konventionen om tillämpning av Schengenavtalet av den 14 juni 1985 (Schengenkonventionen),

– artikel 24 i rådets beslut 2009/917/RIF av den 30 november 2009 om användning av informationsteknik för tulländamål (TIS-rådsbeslutet),

– artikel 33 i rådets beslut av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol),

– artikel 30.5 i rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet),

– artikel 41 i Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen),

– artikel 7.1 och 7.2 i Europaparlamentets och rådets direktiv (EU) 2015/413 av den 11 mars 2015 om underlättande av gräns-

överskridande informationsutbyte om trafiksäkerhetsrelaterade brott (CBE-direktivet), i den ursprungliga lydelsen, *och*

– artikel 8.5 i rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott (VIS-rådsbeslutet).

Paragrafen anger några ytterligare internationella dokument enligt vilka Datainspektionen är nationell tillsynsmyndighet. Ändringen innebär att dataskyddsrambeslutet, som ersätts av det nya dataskyddsdirektivet på det brottsbekämpande området, inte längre är med i denna uppräkning. Ändringen behandlas i avsnitt 9.3.2.

5 §

Myndigheten leds av en myndighetschef, *som anställs genom beslut av regeringen för en period om minst fyra år. Anställningen får förlängas.*

Paragrafen anger att Datainspektionen leds av en myndighetschef. Ändringen innebär att det dessutom föreskrivs att chefen utses av regeringen, att en mandatperiod ska vara minst fyra år och att anställningen kan förlängas. Ändringen behandlas i avsnitt 9.3.3.

Kommittédirektiv 2014:164

En myndighet med ett samlat ansvar för tillsyn över den personliga integriteten

Beslut vid regeringssammanträde den 22 december 2014

Sammanfattning

Ansvaret för tillsyn på integritetsområdet ligger i dag på flera olika myndigheter. I syfte att stärka skyddet för den personliga integriteten ska en särskild utredare överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet. Utredaren ska kartlägga den tillsyn över behandling av personuppgifter som i dag bedrivs av flera myndigheter. I uppdraget ingår även att lämna förslag som medför att myndigheten är förberedd för att kunna fullgöra de uppgifter som Integritetskommittén (Ju 2014:09) kan komma att föreslå att ett integritetsskyddsråd ska ha. Dessutom ska utredaren lämna de förslag som behövs för att myndigheten ska kunna fullgöra de uppgifter som kan bli resultatet av reformeringen av EU:s dataskyddsreglering.

Uppdraget ska redovisas senast den 31 januari 2016.

Den personliga integriteten

Begreppet personlig integritet används både i grundlag och i vanlig lag – t.ex. 2 kap. 6 § andra stycket regeringsformen (RF) och 5 a § personuppgiftslagen (1998:204) – men någon allmängiltig definition av begreppet har inte slagits fast. I ett försök att ändå beskriva

vad som kan anses vara kärnan i rätten till personlig integritet har lagstiftaren uttalat att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas (prop. 2005/06:173 s. 15 och prop. 2009/10:80 s. 175). Rätten till personlig integritet kan också beskrivas som en rätt att bli lämnad i fred eller en rätt till självbestämmande och valfrihet.

Grundläggande bestämmelser om personlig integritet finns bl.a. i regeringsformen. Av målsättningsstadgandet i 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privat- och familjeliv. Vidare finns i 2 kap. 6 § RF en bestämmelse som slår fast ett skydd för förtroliga meddelanden och som även i övrigt ger ett skydd gentemot det allmänna mot betydande intrång i den personliga integriteten som sker utan samtycke och innebär kartläggning eller övervakning av den enskildes personliga förhållanden.

Enligt artikel 8 i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, som gäller som svensk lag, har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Av 2 kap. 19 § RF följer att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen. En bestämmelse om respekt för privat- och familjelivet finns även i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna. Av artikel 8 i stadgan följer vidare att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Rätten till skydd av privatlivet och den personliga integriteten är inte absolut. Rättigheterna kan under vissa förutsättningar således inskränkas.

Pågående utredningsarbete m.m.

Regeringen beslutade i maj 2014 att ge en parlamentariskt sammansatt kommitté – Integritetskommittén (Ju 2014:09) – i uppdrag att utifrån ett individperspektiv kartlägga och analysera sådana företeelser i samhället, inom både privat och offentlig sektor, som kan

medföra faktiska eller potentiella risker för den personliga integriteten och som hänger samman med användningen av modern informationsteknik. Kommittén ska också följa upp effekterna i lagstiftningsarbetet av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes 2011. Vidare ska kommittén överväga behovet av att ge en befintlig myndighet eller ett särskilt inrättat integritetsskyddsråd ett brett och samlat uppdrag att följa utvecklingen på området för den personliga integriteten. Uppdraget ska redovisas senast den 1 december 2016.

Informationshanteringsutredningen (Ju 2011:11) har i uppdrag att bl.a. genomföra en översyn av den s.k. registerlagstiftningen, dvs. regleringen av myndigheternas personuppgiftsbehandling. Uppdraget ändrades i maj 2014 för att anpassas till det pågående arbetet inom EU med ett nytt dataskyddsregelverk. Uppdraget ska redovisas senast den 31 mars 2015.

Vidare har Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten (Ju 2014:10) i uppdrag att göra en bred översyn av det straffrättsliga skyddet för enskildas personliga integritet, särskilt när det gäller hot och andra kränkningar. Utredningen ska redovisa sitt uppdrag senast den 31 januari 2016.

Tillsynen över polisens behandling av personuppgifter utreds av Polisorganisationskommittén (Ju 2010:09) som har i uppdrag att analysera hur tillsynen kan organiseras så att överlappning mellan olika tillsynsmyndigheter i så stor utsträckning som möjligt undviks. Uppdraget är en följd av kommitténs tidigare förslag om en tillsynsmyndighet för polisen. Uppdraget ska redovisas senast den 30 april 2015.

Inom EU pågår en omfattande översyn av regelverket för behandling av personuppgifter. Reformen tar sin utgångspunkt i förslag som Europeiska kommissionen presenterade i januari 2012 (KOM [2012] 10 och KOM [2012] 11). Förslagen innebär bl.a. att 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, som i Sverige har genomförts genom bl.a. personuppgiftslagen, ska ersättas av en allmän uppgiftsskyddsförordning.

Uppdraget

Regeringen har i budgetpropositionen för 2015 aviserat åtgärder för att stärka skyddet för enskildas integritet, såväl i Sverige som i EU. En av dessa åtgärder är att utreda hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur (prop. 2014/15:1, utgiftsområde 4, s. 23).

Det finns för närvarande en rad myndigheter som har till uppgift att tillvarata enskildas intresse av skydd för den personliga integriteten. *Datainspektionen* har, enligt personuppgiftslagen, det övergripande ansvaret att värna skyddet för enskildas personliga integritet vid behandling av personuppgifter. Myndigheten har också tillsynsansvar enligt flera andra lagar på integritetsområdet, bl.a. kameraövervakningslagen (2013:460). Även *länsstyrelserna* har ansvar för tillsyn över kameraövervakning, men det ansvaret begränsar sig till övervakning på platser dit allmänheten har tillträde. Till detta kommer den tillsyn som bedrivs av *Justitiekanslern* och av sektorsspecifika myndigheter som t.ex. *Inspektionen för vård och omsorg*.

Tillsyn över behandlingen av personuppgifter utövas på vissa områden även av andra myndigheter än Datainspektionen. *Post- och telestyrelsen* har i uppdrag att utöva tillsyn vid behandling av uppgifter vid elektronisk kommunikation. Ett annat exempel är *Säkerhets- och integritetsskyddsnämnden* som utövar tillsyn över polisens personuppgiftsbehandling enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister.

Ansvaret för tillsynen på integritetsområdet ligger således på flera myndigheter. Det har i olika sammanhang diskuterats om en myndighet bör ges ett bredare uppdrag inom detta område. Exempelvis förordade Integritetsskyddskommittén en utveckling och breddning av Datainspektionens roll. Kommittén ansåg också att det fanns en brist på systemtänkande och helhetssyn i den integritetsskyddsrättsliga lagstiftningen och att rätten till personlig integritet borde få en mer framskjuten ställning i samhället. Mot bl.a. den bakgrunden bedömde kommittén även att det kunde finnas skäl att i en framtid överväga inrättandet av ett särskilt integritetsskyddsråd med ett brett uppdrag att vaka över integritetsskyddet i dess helhet (SOU 2007:22, del 1, s. 489 f., SOU 2008:3 s. 331 f.). Den frågan tas, som nämnts, om hand av Integritetskommittén.

Frågan om att ge en myndighet ett bredare uppdrag har även behandlats i en rad riksdagsmotioner (t.ex. 2011/12:Ju6, 2013/14:Ju32, 2013/14:K202). Vidare har Datainspektionen i en skrivelse till regeringen (Ju2011/8857/Å) bl.a. tagit upp frågan om gränssnitten mellan olika myndigheter.

Regeringen anser att det, mot den angivna bakgrunden, finns skäl att utreda hur skyddet för enskildas personliga integritet kan förstärkas genom att tillsynen över behandling av personuppgifter i högre grad samlas hos en myndighet. En sådan myndighet bör även ha i uppdrag att lämna förslag till regeringen om eventuella behov av åtgärder för att stärka skyddet för den personliga integriteten när det gäller behandling av personuppgifter.

Med anledning av Integritetskommitténs pågående uppdrag, att överväga inrättandet av ett särskilt integritetsskyddsråd, finns det anledning för utredaren att se över och lämna förslag som medför att myndigheten är förberedd för att kunna fullgöra de uppgifter som det kan komma att föreslås att ett integritetsskyddsråd ska ha. Utredaren måste också förhålla sig till den pågående översynen av EU:s dataskyddsreglering och – så långt som möjligt – lämna de förslag som behövs för att myndigheten ska kunna fullgöra de uppgifter som kan bli resultatet av den översynen.

Utredaren ska därför

- kartlägga den tillsyn över behandling av personuppgifter som i dag bedrivs av flera myndigheter,
- analysera fördelar och nackdelar med att i högre grad samla tillsynen över behandling av personuppgifter hos en myndighet,
- lämna förslag på hur tillsynen – helt eller delvis – kan samlas hos en myndighet samt hur myndighetens uppdrag bör vara utformat och vilka befogenheter myndigheten bör ha för att kunna upprätthålla en effektiv tillsynsverksamhet,
- analysera konsekvenserna för berörda myndigheter när det gäller verksamhet, organisation, resurser och personal,
- lämna förslag som medför att myndigheten är förberedd för att kunna fullgöra de uppgifter som Integritetskommittén kan komma att föreslå att ett integritetsskyddsråd ska ha,

- lämna de förslag som behövs för att myndigheten ska kunna fullgöra de uppgifter som kan bli resultatet av reformeringen av EU:s dataskyddsreglering, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Den granskning av behandling av personuppgifter som bedrivs vid Statens inspektion för försvarsunderrättelseverksamheten omfattas inte av uppdraget.

Genomförande och redovisning av uppdraget

Utredaren ska samråda med Integritetskommittén (Ju 2014:09) och Polisorganisationskommittén (Ju 2010:09). Även i övrigt ska utredaren hålla sig informerad om arbete som bedrivs inom Regeringskansliet och utredningsväsendet på det område som uppdraget avser. Samråd ska även ske med Datainspektionen, Post- och telestyrelsen, Säkerhets- och integritetskyddsnämnden och andra berörda myndigheter och organisationer. Utredaren ska också följa den pågående översynen av EU:s dataskyddsreglering.

I uppdraget ingår att, utifrån de överväganden som görs, lämna fullständiga författningsförslag. Förslagen ska utformas på ett sådant sätt att de, så långt som möjligt, är förenliga med den kommande unionsrättsliga dataskyddsregleringen. Vidare ska förslagen vara så kostnadseffektiva som möjligt ur ett statsfinansiellt perspektiv.

Utredaren är oförhindrad att ta upp närliggande frågor som han eller hon anser behöver övervägas för att uppdraget ska kunna genomföras på ett fullgott sätt.

Utredaren ska i enlighet med kommittéförordningen (1998:1474) redovisa konsekvenserna av sina förslag och vid behov föreslå hur dessa ska finansieras.

Uppdraget ska redovisas senast den 31 januari 2016.

(Justitiedepartementet)

Kommittédirektiv 2015:139

Tilläggsdirektiv till Utredningen om tillsynen över den personliga integriteten (Ju 2015:02)

Beslut vid regeringssammanträde den 17 december 2015

Förlängd tid för uppdraget

Regeringen beslutade den 22 december 2014 kommittédirektiv om hur skyddet för den personliga integriteten kan förstärkas genom att tillsynen över behandling av personuppgifter i högre grad samlas hos en myndighet (dir. 2014:164). Enligt utredningens direktiv skulle uppdraget redovisas senast den 31 januari 2016.

Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 30 september 2016.

(Justitiedepartementet)

Statens offentliga utredningar 2016

Kronologisk förteckning

1. Statens bredbandsinfrastruktur som resurs. N.
2. Effektiv vård. S.
3. Höghastighetsjärnvägens finansiering och kommersiella förutsättningar. N.
4. Politisk information i skolan – ett led i demokratiuppdraget. U.
5. Låt fler forma framtiden! Del A + B. Ku.
6. Framtid sökes – Slutredovisning från den nationella samordnaren för utsatta EU-medborgare. S.
7. Integritet och straffskydd. Ju.
8. Ytterligare åtgärder mot penningtvätt och finansiering av terrorism. Fjärde penningstvättsdirektivet – samordning – ny penningtvättslag – m.m. Del 1 + 2. Fi.
9. Plats för nyanlända i fler skolor. U.
10. EU på hemmaplan. Ku.
11. Olika vägar till föräldraskap. Ju.
12. Ökade möjligheter till modersmålsundervisning och studiehandledning på modersmål. U.
13. Palett för ett stärkt civilsamhälle. Ku.
14. En översyn av tobakslagen. Nya steg mot ett minskat tobaksbruk.S.
15. Arbetsklausuler och sociala hänsyn i offentlig upphandling – ILO:s konvention nr 94 samt en internationell jämförelse. Fi.
16. Kunskapsläget på kärnavfallsområdet 2016. Risker, osäkerheter och framtidsutmaningar. M.
17. EU:s reviderade insolvensförordning m.m. Ju.
18. En ny strafftidslag. Ju.
19. Barnkonventionen blir svensk lag. S.
20. Föräldraledighet för statsråd? Fi.
21. Ett klimatpolitiskt ramverk för Sverige. M.
22. Möjlighet att begränsa eller förbjuda odling av genetiskt modifierade växter i Sverige. M.
23. Beskattning av incitamentsprogram. Fi.
24. En ändamålsenlig kommunal redovisning. Fi.
25. Likvärdigt, rättssäkert och effektivt – ett nytt nationellt system för kunskapsbedömning. Del 1 + 2. U.
26. På väg mot en ny politik för Sveriges landsbygder – landsbygdernas utveckling, möjligheter och utmaningar. N.
27. Som ett brev på posten. Postbefordran och pristak i ett digitaliserat samhälle. N.
28. Vägen till självkörande fordon – försöksverksamhet. N.
29. Trygghet och attraktivitet – en forskarkarriär för framtiden. U.
30. Människorna, medierna & marknaden. Medieutredningens forskningsantologi om en demokrati i förändring. Ku.
31. Fastighetstaxering av anläggningar för el- och värmeproduktion. Fi.
32. En trygg dricksvattenförsörjning. Del 1 + 2 och Sammanfattning. N.
33. Ett bonus–malus-system för nya lätta fordon. Fi.
34. Revisorns skadeståndsansvar. Ju.
35. Vägen in till det svenska skolväsendet. U.
36. Medverkan av tjänsteleverantörer i ärenden om uppehålls- och arbetstillstånd. UD.
37. Rätten till en personförsäkring. – ett stärkt konsumentskydd. Ju.
38. Samling för skolan. Nationella målsättningar och utvecklingsområden för kunskap och likvärdighet. U.

39. Polis i framtiden
– polisutbildningen som högskoleutbildning. Ju.
40. Straffrättsliga åtgärder mot deltagande i en väpnad konflikt till stöd för en terroristorganisation. Ju.
41. Hur står det till med den personliga integriteten?
– en kartläggning av Integritetskommittén. Ju.
42. Ett starkt straffrättsligt skydd mot köp av sexuell tjänst och utnyttjande av barn genom köp av sexuell handling, m.m. Ju.
43. Internationella säkerhetsrätter i järnvägsfordon m.m.
– Järnvägsprotokollet. Ju.
44. Kraftsamling mot antiziganism. Ku.
45. En hållbar, transparent och konkurrenskraftig fondmarknad. Fi.
46. Samordning, ansvar och kommunikation – vägen till ökad kvalitet i utbildningen för elever med vissa funktionsnedsättningar. U.
47. En klimat- och luftvårdsstrategi för Sverige. Del 1 + Del 2, bilaga med underlagsrapporter. M.
48. Regional indelning – tre nya län. Fi.
49. En utökad beslutanderätt för Konkurrensverket. N.
50. Genomförande av sjöfolksdirektivet. A.
51. Villkor för intjänande och bevarande av tjänstepension. A.
52. Färre i häkte och minskad isolering. Ju.
53. Betaltjänster, förmedlingsavgifter och grundläggande betalkonton. Fi.
54. Till sista utposten. En översyn av postlagstiftningen i ett digitaliserat samhälle. N.
55. Det handlar om jämlik hälsa. Utgångspunkter för Kommissionens vidare arbete. S.
56. Ny paketreselag. Fi.
57. Utredningen om Sveriges försvars- och säkerhetspolitiska samarbeten. UD.
58. Ändrade mediegrundlagar. Del 1 + Del 2. Ju.
59. På goda grunder
– en åtgärdsgaranti för läsning, skrivning och matematik. U.
60. Ett starkare skydd för den sexuella integriteten. Ju.
61. Fokus premiepension. Fi.
62. Ökad insyn i välfärden. S.
63. En robust personalförsörjning av det militära försvaret. Fö.
64. Förutsättningar enligt regeringsformen för fördjupat försvarssamarbete. Fö.
65. Ett samlat ansvar för tillsyn över den personliga integriteten. Ju.

Statens offentliga utredningar 2016

Systematisk förteckning

Miljö- och energidepartementet

Kunskapsläget på kärnavfallsområdet 2016. Risker, osäkerheter och framtidsutmaningar. [16]

Ett klimatpolitiskt ramverk för Sverige. [21]

Möjlighet att begränsa eller förbjuda odling av genetiskt modifierade växter i Sverige. [22]

En klimat- och luftvårdsstrategi för Sverige. Del 1 + Del 2, bilaga med underlagsrapporter. [47]

Näringsdepartementet

Statens bredbandsinfrastruktur som resurs. [1]

Höghastighetsjärnvägens finansiering och kommersiella förutsättningar. [3]

På väg mot en ny politik för Sveriges landsbygder – landsbygdernas utveckling, möjligheter och utmaningar. [26]

Som ett brev på posten. Postbefordran och pristak i ett digitaliserat samhälle. [27]

Vägen till självkörande fordon – försöksverksamhet. [28]

En trygg dricksvattenförsörjning. Del 1 + 2 och Sammanfattning. [32]

En utökad beslutanderätt för Konkurrensverket. [49]

Till sista utposten. En översyn av postlagstiftningen i ett digitaliserat samhälle. [54]

Socialdepartementet

Effektiv vård. [2]

Framtid sökes – Slutredovisning från den nationella samordnaren för utsatta EU-medborgare. [6]

En översyn av tobakslagen. Nya steg mot ett minskat tobaksbruk. [14]

Barnkonventionen blir svensk lag. [19]

Det handlar om jämlik hälsa. Utgångspunkter för Kommissionens vidare arbete. [55]

Ökad insyn i välfärden. [62]

Utbildningsdepartementet

Politisk information i skolan – ett led i demokratiuppdraget. [4]

Plats för nyanlända i fler skolor. [9]

Ökade möjligheter till modersmålsundervisning och studiehandledning på modersmål. [12]

Likvärdigt, rättssäkert och effektivt – ett nytt nationellt system för kunskapsbedömning. Del 1 + 2. [25]

Trygghet och attraktivitet – en forskarkarriär för framtiden. [29]

Vägen in till det svenska skolväsendet. [35]

Samling för skolan. Nationella målsättningar och utvecklingsområden för kunskap och likvärdighet. [38]

Samordning, ansvar och kommunikation – vägen till ökad kvalitet i utbildningen för elever med vissa funktionsnedsättningar. [46]

På goda grunder – en åtgärdsgaranti för läsning, skrivning och matematik. [59]

Utrikesdepartementet

Medverkan av tjänsteleverantörer i ärenden om uppehålls- och arbetstillstånd. [36]

Utredningen om Sveriges försvars- och säkerhetspolitiska samarbeten. [57]