dataskydd.net
ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
c/o Anders Lundquist
Eningebölevägen 44
749 61 Örsundsbro

Justitiedepartementet
103 33 Stockholm

Lund 2015-11-21

Remissyttrande över SOU 2015:39 – Myndighetsdatalag

Dataskydd.net avstyrker utredningens förslag till ny myndighetsdatalag. Dataskydd.net lämnar särskilda kommentarer på följande delar av utredningen:

- Kapitel 5 om utlämning, effektivisering och integritet. (s. 3)
- Kapitel 7 om den allmänna bakgrunden. (s. 5)
- Kapitel 8 om allmänna bestämmelser. (s. 9)
- Kapitel 9 om lagens tillämpningsområde. (s. 12)
- Kapitel 10 om personuppgiftsansvar och säkerhet. (s. 16)
- Kapitel 11 om utlämning av personuppgifter. (s. 19)
- Kapitel 12 om överföring till tredje land. (s. 21)
- Kapitel 13 om information till den registrerade. (s. 22)
- Kapitel 14 om arkivering och gallring. (s. 23)
- Kapitel 15 om skyldighet att vidta åtgärder då personuppgifter är oriktiga eller behandlas otillåtet. (s. 23)
- Kapitel 16 om förhållandet mellan tillsynsmyndigheten och myndigheterna i övrigt. (s. 24)
- Kapitel 17 om tillsynsmyndighetens befogenheter. (s. 24)

Dataskydd.net uttrycker fullt stöd för förslagen i kapitel 15. Övriga förslag är behäftade med brister och bör omvärderas.

Texten är strukturerad så att utredningens kvalitet granskas kapitel för kapitel. Då utredarna i Dataskydd.net:s mening gjort felaktiga antaganden i grunden, och bortsett från viktiga konsekvenser av de förpliktelser Sverige har åtagit sig genom sina medlemskap i EU och Europarådet, kommer vissa kommentarer upprepa sig mellan kapitlen.

I bilaga 1 (s. 26–36) finns ett tre-kolumns-dokument som sammanställer samtliga ursprungsförslag, ändringsförslag samt kortfattade kommentarer till ändringsförslagen. För längre motiveringar av ändringsförslagen hänvisas till brödtexten och källhänvisningar i brödtexten.

Texten kan läsas som fristående text men är i grunden menad att vara en kommentar på utredningen om en ny myndighetsdatalag (SOU 2015:39). Vid de

tillfällen då det är extra viktigt för förståelsen av texten att kunna hänvisa tillbaka till utredningen finns sidhänvisningar angivet i marginalnoter. Detta gäller också vid de tillfällen då Dataskydd.net dragit paralleller mellan den innevarande utredningen och tidigare statliga alster på området.

Inledning

SOU 2015:39, kapitel 4

Dataskydd.net är positiva till att utredningen tar upp problemen med de komplexa registerförfattningarna. Vi ser inga anledningar att ifrågasätta att det blir svårare för enskilda privatpersoner och för myndigheter att bena ut vad individernas rättigheter egentligen är i det spretiga regelverk som finns i dag. Dataskydd.net välkomnar också att man problematiserat uppdelningen mellan olika utlämningsförfaranden för uppgifter (direktåtkomst och annat elektroniskt utlämnande).

SOU 2015:39, kapitel 5

Det verkar dock som att utredarna fastnat i teknisk determinism. Juridiken är inte ett verktyg som kan skydda privatpersonen *trots* tekniken. Tekniken kan tvärtom genom incitament som uppstår ur en väl övervägd juridik designas på ett sådant sätt att privatpersonen skyddas *med hjälp av* tekniken. Sådan utveckling finns i viss omfattning redan: till exempel investerar myndigheter redan i loggningssystem och accesskontroller. Sådana tekniska lösningar kan användas för att tillgodose utredarnas krav på sökbegränsningar, men de skulle också kunna vara ett transparensverktyg för privatpersoner.

Utredningen har skett på myndigheternas villkor. Transparensverktyg som tillfaller privatpersoner för att granska databehandling hos myndigheter diskuteras till exempel utifrån perspektivet att de kan vara ett problem för myndigheten. I dagsläget är problemet för varje enskild privatperson snarare att loggning och accesskontroll görs av myndighetscentrerade säkerhetsbetänkelser snarare än individcentriska dataskyddsskäl. Om privatpersonerna inte själva bereds tillgång till information om hur deras information och uppgifter behandlas, kan de inte utkräva ansvar av myndigheter som kränker deras integritet. Privatpersonens möjlighet att aktivt utöva sina rättigheter borde vara centralt för myndigheterna, inte sättas i baksätet.

SOU 2015:39, s. 23, s. 59, s. 85, s. 109, s. 118, s. 131, s. 149

Effektivitet ställs i motsatsförhållande till integritet. Dataskydd.net delar inte problemformuleringen att effektivitet och dataskydd står i motsats till varandra. Mycket teknisk utveckling syftar idag till att ge privatpersoner bättre inflytande över både sig själv och sin situation relativt andra. Det vore olyckligt om myndighetsdatalagen ger incitament för entreprenörer inom offentlig förvaltning att inte haka på den utvecklingen.

Lagförslagen i utredningens kapitel 1 definierar en passiv privatperson som inte själv har något med utövandet av sina rättigheter att göra. Om man i stället förutsätter en aktiv privatperson som har kapacitet att själv utöva sina rättigheter kan man formulera lagförslagen på ett mindre preskriptivt sätt. En öppnare lagstiftning lämnar öppet för fler tekniska utvecklingar i framtiden.

Kapitel 5: Avstyrker utredningens bedömningar om utlämnande, effektivisering och integritet.

Dataskydd.net uppfattar utredarnas bedömning av behovet av en åtskillnad mellan direktåtkomst och annat elektroniskt utlämnande som olycklig. Tillräck-

ligt förtroende utsträcks inte till att tekniska lösningar går att finna på problem som uppstår då information delas mellan myndigheter. Det leder till en onödigt preskriptiv reglering av vissa utlämningsförfaranden (direktåtkomst). Andra utlämningsförfaranden lämnas i stort sett oreglerade, då det finns en ”presumtion för att ett utlämnande av personuppgifter [från en myndighet] till en annan myndighet inte innebär någon risk för kränkningar av enskildas integritet.”

SOU 2015:39, s. 449

Uppdelningen mellan de olika utlämningsformerna har tillkommit på grund av föreställningen att ”möjligheten till direktåtkomst ökar riskerna för intrång i den personliga integriteten, eftersom det typiskt sett innebär att uppgifter blir tillgängliga för fler personer och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar.” Samtliga utlämningar av uppgifter mellan myndigheter sker dock under relativ brist på transparens, eftersom det finns en föreställning om att individer inte själva kan ta ansvar för eller förstå databehandling hos myndigheter.

SOU 2015:73, s. 304

En aktiv och förstående individ?

Dataskydd.net vill lyfta två saker:

1. Då Sverige skrev under Europeiska konventionen för mänskliga rättigheter tillerkände svenska staten privatpersoner på svenskt territorium individuella rättigheter så som beskrivna i konventionen. Rättigheterna är individuella och tillfaller privatpersoner. Konventionen beskriver statens skyldigheter att säkerställa sig om att individer har möjlighet att åtnjuta dessa rättigheter.
2. Då individer har tillerkänts sådana rättigheter som finns nedskrivna i Europeiska konventionen, behövs det också meningsfulla metoder för individer att utöva dessa rättigheter.

Verktyg som dataminimering och samtycke används för att uppnå rätt balans mellan privatpersonens rättigheter och myndigheternas elektroniska förvaltning. Bättre information till privatpersoner om innevarande tekniska och organisatoriska lösningar hos myndigheten i kombination med tillgång för privatpersonen till effektiva rättsmedel (till exempel möjlighet att få skälig ersättning vid överträdelser samt införandet av en ombudsmannafunktion) skulle bidra till en stabilare och säkrare elektronisk förvaltning, som också upprätthåller och stärker privatpersoners mänskliga rättigheter.

I Sverige har möjligheter för individer att själva utöva sina rättigheter saknats. Tillsynen är i princip begränsad till Datainspektionen, och möjligheten att få skadestånd begränsad. Vad gäller dataskydd är detta särskilt graverande för individen, eftersom de faktorer som ofta förhindrar myndigheter från att göra investeringar i bättre dataskydd coh datasäkerhet är av ekonomisk art. Det finns i princip två saker lagstiftaren kan göra för att ge starkare incitament till myndigheterna att ta dataskydd och datasäkerhet på större allvar. Det ena är att göra bristande förmåga att fokusera på dessa aspekter ekonomiskt kostsamt. Det andra är att se till att privatpersoner får reda på och kan skapa negativ uppmärksamhet för myndigheten kring eftersättande av privatpersonens rättigheter.

Utredarnas syn på utlämningsbegreppet och integritetsskydd förefaller snarare utgöra en fortsättning på mönstret att individens roll i utövande av rättigheten bör vara begränsad. Om utgångspunkten i stället är en aktiv privatperson som själv kan tilldelas en roll vid upprätthållandet av dess egna rättigheter, blir regleringen av utlämning mycket enklare. För mer läsning om detta hänvisar vi till våra kommentarer på kapitel 9, 10, 11, 13 och 17 nedan.

Vad är ett integritetsintrång?

Det står inte klart att utlämnande av uppgifter genom direktåtkomst innebär ett större intrång i integriteten än utlämnande av uppgifter som sker på något annat sätt. Bara den omständighet att en viss handling är eller inte är sekretessklassad

kan inte anses fullständigt beskriva de integritetskränkningar som kan uppstå vid behandling av uppgifterna. Det är således felaktigt att anta att direktåtkomst per definition utgör en högre risk för integritetsintrång än annat utlämnande eller behandling, och detta borde särskilt vara fallet efter det att Högsta förvaltningsdomstolen begränsat begreppet direktåtkomst till sådana utlämningar som rör allmänna handlingar.[1]

HFD, Mål nr 1356-14

Utredarna har förutsatt att staten per definition inte kan utsätta individer för integritetskränkningar, trots att Europeiska konventionen är skriven specifikt för att begränsa staters kränkningar av individers integritet. Även regeringsformen innehåller skrivelser för att begränsa integritetsintrång utförda av staten mot individen.

SOU 2015:39, s. 198, 207, 449

SOU 2015:39, s. 61

SOU 2015:39, s. 66

Kapaciteten för icke-statliga aktörer att samköra register har ökat. Det gör att en statlig datareglering behöver förhålla sig inte bara till integritetskränkningar som staten och myndigheterna själva kan orsaka, utan även till integritetskränkningar som kan uppstå utanför myndigheternas egna verksamhet till följd av myndigheternas hantering av personuppgifter. En positiv skyldighet för staten att skydda privatpersoners privatliv även utanför den egna verksamheten följer av Europeiska konventionen för mänskliga rättigheter och av Europeiska unionens stadga.

SOU 2015:39, kapitel 3.2.1

”Profilering” är ett samlingsbegrepp för åtgärder som stoppar in individer i olika kategorier och grupptillhörigheter beroende på preferenser och individuella förutsättningar. Profilering kan till exempel vara att man behandlas på ett särskilt sätt för att man är kvinna i en viss åldergrupp, eller att man är man av särskild etnisk härkomst med folkbokföringsadress på en viss plats. Åtgärden syftar ofta till att kunna särbehandla individen baserat på dess grupptillhörighet. Det rör sig om positiv eller negativ diskriminering till följd av automatisk databehandling.

Det finns omfattande forskning på diskriminerande effekter av profilering i samband med till exempel marknadsföring,[2] men också ett ökande fokus i forskningen på tillfällen då profilering används för att bevara och befästa rådande normer och stereotyper.[3] Samtidigt finns ett ökande politiskt fokus på profileringstekniker i samband med ”nudging” (knuffning), som innebär att man medelst profilering och belöningar uppmuntrar människor att bete sig på ett sätt som man upplever är bättre för människorna än om de hade fått bete sig

[1] https://dataskydd.net/nyheter/2015/11/02/hogsta-forvaltningsdomstolen-skapar-flodvag-av-hemlig-datadelning

[2] Hildebrandt, Mireille, Gutwirth, Serge (red.). *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Springer Verlag, 2008; Zuiderveen Borgesius, Frederik J., *Improving privacy protection in the area of behavioural targeting*, doktorsavhandling, Universiteit van Amsterdam, 2014; Schrage, Michael. *Big Data's Dangerous New Era of Discrimination*, Harvard Business Review, 29 januari 2014; Bria, Francesca, Clavell, Gemma Galdon, Ruiz, Javier, Zaala, José María, Fitchner, Laura, Halpin, Harry. *D-CENT: Research on digital identity ecosystems*, NESTA, 2015. Tillgänglig på http://www.nesta.org.uk/publications/d-cent-research-digital-identity-ecosystems

[3] Det finns omfattande material om detta, men för ett nyligt exempel på profilering som påverkar arbetssökande kvinnor negativt, se Datta, Amit, Tschantz, Michael Carl, Datta, Anupam. *Automated Experiments on Ad Privacy Settings – A Tale of Opacity, Choice, and Discrimination.* Proceedings on Privacy Enhancing Technologies. Volume 2015, Issue 1, Pages 92–112, ISSN (Online) 2299-0984, DOI: 10.1515/popets-2015-0007, april 2015

som de annars skulle ha gjort.[4] Vi återkommer både i kommentarerna på kapitel 7.

Sammantaget upplever inte Dataskydd.net att man, som utredningen, kan begränsa diskussionen om utlämning av personuppgifter från myndigheter till ett fåtal juridiska specialfall. En juridisk uppdelning av ansvarsfunktioner och utlämningsmetoder som sedan ändå inte kan granskas av dem som uppdelningen är ämnad att skydda, menar Dataskydd.net förbiser både integritetsproblem som uppstår i elektroniska system och förutsättningarna för en optimal användning av modern informationsteknologi.

Vad gäller överskottsinformation vid utlämnande, den enda integritetsrisk som utredningen konkretiserar, är Dataskydd.net av uppfattningen att en sund risk- och ansvarsfördelning, samt adekvat transparens och möjlighet till ansvarsutkrävande för privatpersoner, på sikt skulle leda till en rättsutveckling och teknisk utveckling sådan att problem som kan följa av sådant utlämnande ändå skulle åtgärdas.

För vidare behandling av dessa frågor hänvisas till kommentarerna på kapitel 9-11, 13 och 15.

Dataskydd.net förordar en modell där individen ges stor insikt och möjlighet att påverka hur information delas mellan olika myndigheter, och även en möjlighet till effektiva rättsmedel vid tillfällen då individen upplever att utlämning har skett i strid mot några enkla, men grundläggande principer, enligt följande principer:
1. Individcentrering
2. Rätt att veta
3. Rätt att samtycka
4. Dataminimering
5. Skälig ersättning vid kränkning

Kapitel 7: Avstyrker utredningens bedömningar om den allmänna bakgrunder

Dataskydd.net avstyrker utredningens bedömningar. De är motstridiga och missar att göra en adekvat analys av integritetsaspekter. Utredningen är alltså ingen skillnad mot, utan en bekräftelse av, Integritetsutredningens påstående att ”[integritetsskyddet] rent allmänt värdera[s] förhållandevis lågt i lagstiftningen”. SOU 2008:8, s. 191

Utredarna konstaterar att ”den elektroniska förvaltningen är ju inte längre någon särskild del av myndigheternas verksamhet, utan utgör i själva verket förvaltningen” men samtidigt att ”utgångspunkt för arbetet med en generell reglering om myndigheters behandling av personuppgifter bör vara att den inte till någon del ska syfta till att reglera en myndighets verksamhet.” Senare skrivs att ”[p]ersonuppgiftsbehandling är en integrerad del i myndigheternas utförande av sina författningsreglerade uppgifter och befogenheter.” SOU 2015:39, s. 176 SOU 2015:39, s. 178 SOU 2015:39, s. 601

Utredarna utgångspunkt är att den databehandling som utgör förvaltningens verksamhet inte ska täckas av dataskyddsbestämmelser. Det leder förvisso till att ”regelverket blir tydligare i den meningen att det klargörs vad som utgör ett berättigat dataskydd och hur detta ska åstadkommas på myndighetsområdet”. Däremot kan det knappast antas främja integritetsskyddet och privatpersoners rättigheter. Om myndigheternas verksamhet är beroende av personuppgiftsbehandling, är det rimligt att verksamheten (och de IT-system som möjliggör verksamheten) måste förhålla sig till dataskydd. Vi vill att myndigheternas verksamhet ska utformas så att den garanterar, inte hamnar i motsatsställning till, mänskliga rättigheter. SOU 2015:39, s. 178

För att observera privatpersoners rätt till dataskydd och det allmänna in-

[4] Återigen finns både generella och specifika exempel, och många studier, men följande exempel på hur man kan manipulera känslotillståndet hos grupper av användare i sociala nätverk är illustrativt: Kramer, Adam D. I. Kramer, Guillory, Jamie E. Guillory, Hancock, Jeffrey T. *Experimental evidence of massive-scale emotional contagion through social networks*. Proceedings of the National Academy of Sciences of the United States of America. Tillgänglig på http://www.pnas.org/content/111/24/8788.full; Alonso, Martin Liby. *Dubbel svensk hemläxa*. DN, 26 juli 2015. Tillgänglig på http://www.dn.se/ledare/signerat/martin-liby-alonso-dubbel-svensk-hemlaxa/

tresset av datasäkerhet krävs att de juridiska lösningarna för e-förvaltningen är utformade på ett sådant sätt att både verksamheten och tekniken tillåter säkerhet och dataskydd. Detta observeras i till exempel i Dataskyddsdirektivet från 1995, och i personuppgiftslagen 31 § om lämpliga tekniska och organisatoriska säkerhetsåtgärder.

Direktiv 95/46/EG, Avdelning VIII

Det krävs också att individen har effektiva medel att skydda sina rättigheter. Dessa medel kan vara möjligheten att få tillräcklig information för att bedöma om dataskyddet faktiskt är tillräckligt i teknisk och organisatorisk bemärkelse. De faktorer som ofta förhindrar myndigheter från att göra investeringar i bättre dataskydd coh datasäkerhet är av ekonomisk art. Det finns i princip två saker lagstiftaren kan göra för att ge starkare incitament till myndigheterna att ta dataskydd och datasäkerhet på allvar. Det ena är att göra bristande förmåga att fokusera på dessa aspekter ekonomiskt kostsamt. Det andra är att se till att privatpersoner får reda på och kan skapa negativ uppmärksamhet för myndigheten kring eftersättande av privatpersonens rättigheter (i princip orsaka ett förtroendetapp för myndigheten om den inte följer lagstiftningen och upprätthåller individuella rättigheter).

Europaparlamentet, A7-0402/2013, Art 5(ea).

Utredarna drar slutsatsen att ”det torde höra till undantagen att en behandling av personuppgifter sedd för sig kan anses utgöra ett ingrepp i enskildas personliga förhållanden”, och skriver att ”det inte kan anses givet att en behandling av känsliga personuppgifter som tillåts med hänsyn till ett viktigt allmänt intresse utgör ett intrång i den enskildes personliga integritet.”

SOU 2015:39, s. 198

SOU 2015:39, s. 207

Att behandling av uppgifter som sådan, eller att behandling av känsliga uppgifter hos myndigheter, skulle undantas från omfånget av individuella rättigheter är felaktigt i förhållande till Sveriges internationella förpliktelser. Europeiska dataskyddstillsynsmannen har anfört att dataskydd är den process genom vilken individer kan säkerställa det privatliv och det integritetsskydd som de har rätt till enligt Europeiska konventionen för mänskliga rättigheter artikel 8 och EU:s stadga för grundläggande rättigheter i artikel 7.[5] Synsättet har stöd i Europarådets konvention om dataskydd från 1981.[6] Att bortse ifrån eller förminska det verktyg varigenom individer utövar rättigheter är emellertid också principiellt fel.

SOU 2015:39, kapitel 3.2.1

EDPS Pleading before the General Court in Case C-615/13P

Behandling av personuppgifter handlar ofta om en avvägning mellan det allmännas intresse, kommersiella intressen och individuella intressen. Sättet på vilket man hanterar dessa avvägningar är inte genom att förneka dem, utan genom att synliggöra dem och diskutera dem. Statliga offentliga utredningar har här ett särskilt ansvar att synliggöra avvägningarna för lagstiftaren, så att lagstiftaren kan fatta relevanta beslut utifrån sina egna värderingar och förutsättningar.

Utöver individens intresse av att ha en förutsägbar och transparent databehandling, med tillhörande medel för att utkräva ansvar vid fel och överträdelser,

[5] Se till exempel EDPS Pleading before the General Court in Case C-615/13P *Client Earth and Pan Europe v EFSA*, Luxembourg, 22 January 2015. Tillgänglig på https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-01-22_EDPS_Pleading_Client_Earth_and_Pan_Europe_v_EFSA_EN.pdf

[6] European Treaty Series – No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Artikel 1: ”*The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (”data protection”).*”

finns ett samhälleligt intresse av att individer har denna möjlighet att ta hand om sig själva. ”Profilering” är ett samlingsbegrepp för åtgärder som stoppar in individer i olika kategorier och grupptillhörigheter beroende på preferenser och individuella förutsättningar. Profilering kan till exempel vara att man behandlas på ett särskilt sätt för att man är kvinna i en viss åldergrupp, eller att man är man av särskild etnisk härkomst med folkbokföringsadress på en viss plats. Åtgärden syftar ofta till att kunna särbehandla individen baserat på dess grupptillhörighet. Det rör sig alltså om positiv eller negativ diskriminering till följd av automatisk databehandling.

Det finns omfattande forskning på diskriminerande effekter av profilering i samband med till exempel marknadsföring[7], men också ett ökande fokus i forskningen på tillfällen då profilering används för att bevara och befästa rådande normer och stereotyper.[8] Samtidigt finns ett ökande politiskt fokus på profileringstekniker i samband med ”nudging” (knuffning), som innebär att man medelst profilering och belöningar uppmuntrar människor att bete sig på ett sätt som man upplever är bättre för människorna än om de hade fått bete sig som de annars skulle ha gjort.[9]

Viss profilering är vanligt även på svenska myndigheter. Vissa åldersgrupper, till exempel barn eller föräldrar till barn, får särskilda förmåner från offentlig sektor. Statlig profilering kan också ta sig mer extrema uttryck. I andra länder, till exempel Storbritannien, har man särskilda enheter som fokuserar bara på att behandla information om individers grupptillhörigheter och preferenser, i syfte att få bättre verktyg för att uppmuntra människor att acceptera regeringens och myndigheternas verksamheter.[10]

Det europeiska forskningsprojektet D-CENT har kartlagt i djupare detalj hur olika former av ”nudging” används, även för politiska beslut.[11] Notera också en ökad problematisering av begreppet ”smarta städer” som lånar mycket legitimitet från möjligheten att flytta fattandet av beslut från tjänstemän till

[7] Hildebrandt, Mireille, Gutwirth, Serge (red.). *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Springer Verlag, 2008; Zuiderveen Borgesius, Frederik J., *Improving privacy protection in the area of behavioural targeting*, doktorsavhandling, Universiteit van Amsterdam, 2014; Schrage, Michael. *Big Data's Dangerous New Era of Discrimination*, Harvard Business Review, 29 januari 2014; Bria, Francesca, Clavell, Gemma Galdon, Ruiz, Javier, Zaala, José María, Fitchner, Laura, Halpin, Harry. *D-CENT: Research on digital identity ecosystems*, NESTA, 2015. Tillgänglig på http://www.nesta.org.uk/publications/d-cent-research-digital-identity-ecosystems

[8] Det finns omfattande material om detta, men för ett nyligt exempel på profilering som påverkar arbetssökande kvinnor negativt, se Datta, Amit, Tschantz, Michael Carl, Datta, Anupam. *Automated Experiments on Ad Privacy Settings – A Tale of Opacity, Choice, and Discrimination*. Proceedings on Privacy Enhancing Technologies. Volume 2015, Issue 1, Pages 92–112, ISSN (Online) 2299-0984, DOI: 10.1515/popets-2015-0007, april 2015

[9] Återigen finns både generella och specifika exempel, och många studier, men följande exempel på hur man kan manipulera känslotillståndet hos grupper av användare i sociala nätverk är illustrativa: Kramer, Adam D. I. Kramer, Guillory, Jamie E. Guillory, Hancock, Jeffrey T. *Experimental evidence of massive-scale emotional contagion through social networks*. Proceedings of the National Academy of Sciences of the United States of America. Tillgänglig på http://www.pnas.org/content/111/24/8788.full; Alonso, Martin Liby. *Dubbel svensk hemläxa*. DN, 26 juli 2015. Tillgänglig på http://www.dn.se/ledare/signerat/martin-liby-alonso-dubbel-svensk-hemlaxa/

[10] Behavioural insights team. Tillgänglig på https://www.gov.uk/government/organisations/behavioural-insights-team

[11] Bria, Francesca, Clavell, Gemma Galdon, Ruiz, Javier, Zaala, José María, Fitchner, Laura, Halpin, Harry. *D-CENT: Research on digital identity ecosystems*, NESTA, 2015. Tillgänglig på http://www.nesta.org.uk/publications/d-cent-research-digital-identity-ecosystems

algoritmer.[12]

Tyvärr har utredarna valt att inte bara bortse ifrån de samhälleliga implikationer som databehandling, samkörning och bristande inflytande från individen över sin egen identitet kan ha, utan också helt undantagit automatiskt beslutsfattande från omfattningen av sitt förslag. Då EU-domstolen påtalade i sitt beslut om utlämning av personuppgifter mellan rumänska myndigheter av den 1 oktober 2014 att ”lag /…/ [inte], i den mening som avses i artikel 10 i direktiv 95/46, anses utgöra en information som de registrerade berörda redan känner till och som gör att den registeransvarige befrias från sin skyldighet att informera /…/ personer”, måste denna slutsats från utredarna i dag anses vara förlegad. Vi återkommer till detta i kommentarerna på kapitel 9.

SOU 2015:39, s. 242

C-201/14 – Bara m.fl., p. 38

Dataskydd.net vill ägna några särskilda ord åt begreppet ”effektivitet”. Utredningen tar upp att ytterligare effektiviseringar av förvaltningen medelst modern informationsteknologi bör tillåtas äga rum. Effektivitet ställs i motsatsförhållande till integritet: utredningen presenterar effektiviseringsvinster *och* integritetsrisker, som om att dessa alltid går hand i hand.

SOU 2015:39, s. 23, 59, 85, 109, 118, 131, 149

Att beslut inte dröjer för länge är så klart en viktig del i rättssäkerheten. Det är emellertid inte, så vitt Dataskydd.net förstår, fastlagt att mer datadelning leder till snabbare beslut i bemärkelsen att förtroendet för myndigheterna stärks. Elin Wihlborg vid Linköpings universitet[13] antyder snarare det är *bättre grundade* beslut man är ute efter till följd av mer datadelning. Denna uppfattning får stöd i Riksrevisionens rapport RiR 2010:18[14], där det står ”’[d]e förslag till förbättringar av informationsutbytet som framkommit genom granskningen, skulle innebära en avsevärd effektivisering i form av billigare handläggning, färre fel och bättre service.” Frågan skulle alltså kunna vara om förtroendet för myndigheter gått upp i takt med att mer datadelning sker så att dessa bättre grundade beslut kan ske. Förtroendet för myndigheter Riks-SOM-undersökningen 1986-2007[15] verkar ange att förtroendet långsiktigt snarare minskat.

RiR 2010:18, s. 63

De studier om effektivitet vid distansbetjäning från myndigheterna mot medborgarna visar snarare att organisatoriska brister bortom privatpersonens kontroll gör systemen ineffektiva.[16] Även Statskontoret har indikerat att behovet av arbetskraft och arbetstid på myndigheterna snarare går uppåt än nedåt.[17] Fler IT-system och bättre informationsdelning mellan myndigheterna har få förutsättningar att åtgärda organisatoriska problem. Givet att investeringar i e-förvaltning de senaste åren gått upp, finns ingen anledning att anta en korrelation mellan effektivisering och mer datadelning.

[12] ”*As the tech companies bid for contracts, Haque observed, the real target of their advertising is clear: “The people it really speaks to are the city managers who can say, ‘It wasn’t me who made the decision, it was the data.’”*”. Poole, Steven. *The truth about smart cities: ‘In the end, they will destroy democracy’*, The Guardian, december 2014. Tillgänglig på http://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase

[13] Wihlborg, Elin. Digital government as a guardian of impartiality (?) – Automated public e-services and its implications on Quality of Government, s. 19. European Group of Public Administration, 2015. Tillgänglig på http://liu.diva-portal.org/smash/get/diva2:849243/FULLTEXT01.pdf

[14] http://www.riksrevisionen.se/PageFiles/2086/Anpassad10_18Informationsutbytemellanmyndighetermedansvarförtrygghetssystem.pdf

[15] Förtroendet för myndigheter Riks-SOM-undersökningen 1986-2007. SOM-rapport nr 2008:25

[16] Inspektionen för socialförsäkringen, Rapport 2015:7, Onödig efterfrågan inom Försäkringskassan (Slutrapport), 2014. Tillgänglig på http://www.inspsf.se/digitalAssets/2/2174_rapport_2015-7_web.pdf

[17] Förändringar i svensk statsförvaltning och framtida utmaningar, Statskontoret, 2015. s. 59

Snarare befäster informationsteknologiska system organisatoriska förutsättningar extra hårt: om många tjänstemän är beroende av en viss applikation på ett visst sätt för sina vardagliga sysslor blir applikationen svår att ändra. Om ett tekniskt system visar sig vara osäkert eller dåligt anpassat för att skydda individers integritet kan det av både tekniska och organisatoriska skäl ändå visa sig vara svårt att ändra. Jämför svårigheten med att byta ett databassystem[18] eller att införa nya mjukvarulösningar i verksamheten i övrigt.

Datadelning som gör det svårare för privatpersoner att utöva sina individuella rättigheter verkar också motiveras med att det kan utgöra en kontrollåtgärd mot myndigheternas tjänstemän. Riksrevisionen skriver att ”bristande informationsutbyt[e] leder /…/ till ökad risk för felaktiga utbetalningar, eftersom den manuella kontrollen är så tidskrävande för handläggarna att de ibland väljer att avstå från att göra den,” som om att effektivitetsproblemet handlar om tjänstemän med bristande moral. Man kan så klart betrakta staten och dess myndigheter ur maskinistisk synvinkel, och förvänta sig deterministiska resultat ur varje myndighetsprocess.[19] Detta perspektiv hamnar med nödvändighet i konflikt med privatlivs- och dataskyddsrättigheterna eftersom dessa är konstruerade för att skydda det individualistiska och privatpersoners självbestämmande[20] – även då individerna utgör en del av en större organisation, till exempel en stat. Jämför VAB-reformen som genomfördes 2012-2013 för att underlätta för föräldrar och spara administrationskostnader hos Försäkringskassan – den har lett till något fler felaktiga utbetalningar,[21] men nyttan av reformen kan sammantaget ändå ha uppnått sitt mål (det borde utredas).

RiR 2010:18, s. 63

Dataskydd.net menar att det inte finns något motsatsförhållande mellan effektivitet och dataskydd. Framför allt menar vi att de mänskliga rättigheterna är förutsättningar för en effektiv demokrati. Det är felaktigt att eftersätta och nedprioritera dataskydd av anledningen att man hoppas uppnå bättre förutsättningar för satsningar på moderna informationsteknologiska system. Snarare bör man utforma lagstiftningen så att moderna informationsteknologiska system utvecklas som bättre tillgodoser individuella rättigheter.

Kapitel 8: Avstyrker utredningens förslag på allmänna bestämmelser

Dataskydd.net avstyrker utredningens förslag till syfte. Dataskydd.net avstyrker även förslaget om lagens tillämpningsområde. Dataskydd.net stöder delvis det föreslagna förhållandet mellan personuppgiftslagen och myndighetsdatalagen. Enhetliga definitioner är till exempel bra, och i de fall där personuppgiftslagens skydd är starkare än myndighetsdatalagens skydd föreslår Dataskydd.net att man använder sig av personuppgiftslagens bestämmelser i stället för de av utredningen föreslagna bestämmelserna.

I bilaga 1 finns ett tre-kolumns-dokument som sammanställer förslag från

[18] Jämför brittiska regeringens längre tids försök att göra sig själva mindre beroende av databasjätten Oracle. I augusti 2015 tecknades, tvärtom flera års tidigare viljeyttringar, i stället ett utökat avtal med den leverantör man försökt befria sig från: https://thestack.com/cloud/2015/08/20/uk-government-signs-new-deal-with-oracle/

[19] För en intressant teknikhistorisk behandling av denna tankeströmning i Storbritannien, se Agar, Jon. *The Government Machine – A Revolutionary History of the Computer*. MIT Press, 2003.

[20] Se till exempel Hildebrandt, Mireille, O’Hara, Kieron, Waidner, Michael *Introduction* i *Digital Enlightenment Yearbook 2013 - The Value of Personal Data* om målsättningar för en rätt till privatliv.

[21] Se till exempel https://www.gp.se/nyheter/sverige/1.2884301-fler-aker-fast-for-vab-fusk

utredningen, Dataskydd.net:s ändringsförslag samt kortfattade kommentarer till ändringsförslagen. Brödtexten nedan ger en bredare kontext till Dataskydd.net:s förslag.

Syfte

Utredarna föreslår ett tudelat syfte. Det första syftet gagnar myndigheten. Det andra syftet skyddar människor mot kränkning av deras personliga integritet. Syftet beskriver privatpersonen som passiv, någon som behöver skyddas. Myndigheter ges en aktiv roll: de får möjligheter att göra det som krävs. Människan ses inte som en aktiv människa som själv kan bidra och agera i processen att förvalta människans rättigheter. Dataskydd.net förordar i stället en modell där individen tilldelas en aktivare roll i förvaltningen av sig själv, och där individen ges meningsfulla möjligheter att samverka och invända mot de handlingar som myndigheterna vidtar.

Enligt EU:s stadga för grundläggande mänskliga rättigheter är dataskydd en rättighet som tillfaller varje individ, och som det behöver finnas effektiva rättsmedel för att upprätthålla. Europeiska dataskyddstillsynsmannen har anfört att dataskydd är den process genom vilken individer kan säkerställa det privatliv och det integritetsskydd som de har rätt till enligt Europeiska konventionen för mänskliga rättigheter artikel 8 och EU:s stadga för grundläggande rättigheter i artikel 7.[22] Synsättet har stöd i Europarådets konvention om dataskydd från 1981.[23]

EU-stadgan, artikel 8 och 47.

Dataskydd.net tror att utredarnas slutsatser grundas i att utredarna förutsätter att staten inte kan utsätta individer för integritetskränkningar, trots att Europeiska konventionen är skriven specifikt för att begränsa staters kränkningar av individers integritet. Även regeringsformen innehåller skrivelser för att begränsa integritetsintrång utförda av staten mot individen.

SOU 2015:39, s. 198, 207, 449
SOU 2015:39, s. 61
SOU 2015:39, s. 66

Tillämpningsområde

Personuppgiftsansvaret är en av många delar i den svenska dataskyddsrätten där den juridiska föreställningen inte motsvarar en teknisk verklighet. Uppdelningen av ansvar mellan personuppgiftsansvariga och personuppgiftsbiträden är förlegad[24,25] och inför EU:s dataskyddsreform riktades kritik mot uppdelningen.[26]

I slutändan finns uppdelningen kvar i EU-kommissionens förslag, men personuppgiftsbiträden ges betydligt större skyldigheter att säkerställa sig om att personuppgiftsansvarig ställer sådana krav att personuppgiftsansvarig kan uppfylla sina förpliktelser. EU-kommissionen har också föreslagit en separat möjlighet att söka skadestånd och utdöma viten mot personuppgiftsbiträden som inte bidrar till att dataskyddslagstiftningens regler upprätthålls.

KOM(2012)11, Art 26(2)(f).
KOM(2012)11, Art 75, 77.

[22] Se ovan fotnot 5.
[23] Se ovan, fotnot 6.
[24] Traung, Peter. *The Proposed New EU General Data Protection Regulation*, Computer Law Review International. Volume 13, Issue 2, Pages 33–49, september 2013
[25] Artikel 29-gruppen. Opinion 3/2010 on the principle of accountability, juli 2010, p. 46. Tillgänglig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf
[26] EU-kommissionen, DG Justice, enhet C.3: dataskydd. *Summary of replies to the public consultation about the future legal framework for protecting personal data*. November 2010. Tillgänglig på http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

Utredarna föreslår i stället att personuppgiftsbiträden precis som hittills inte ska ges några skyldigheter att vidta sådana åtgärder som hjälper personuppgiftsansvarig att skydda privatpersoners rättigheter. I stället hamnar allt ansvar fortsatt på personuppgiftsansvarig. Utredarna tycks motivera detta med risken för att personuppgiftsansvariga och personuppgiftsbiträden annars skulle skylla på varandra, vilket skulle leda till sämre möjligheter för privatpersonen att kräva ersättning vid kränkning. Det är emellertid en juridisk-teknisk invändning, som går att lösa med bättre tillgänglighet till information och ömsesidiga förpliktelser på ansvariga och biträden att hjälpa varandra skydda individens rättigheter, eller en möjlighet att bedriva parallella processer.[27] Även i den nuvarande skadeståndsbestämmelsen i personuppgiftslagen finns en möjlighet för personuppgiftsansvarig att begära jämkning om denne kan påvisa att kränkningen inte var dennes fel. Det vore oönskvärt om ingen kan hållas ansvarig ifall den personuppgiftsansvarige kan hänvisa till ett biträde som, till exempel, inte tillhandahåller någon annan teknisk lösning än den kränkande.

Förslag till myndighetsdatalag, 3 §

Förslag till myndighetsdatalag, 20-21 §§

SOU 2015:39, s. 639

Utredarnas förslag följer regeringens proposition 2014/15:148 om en ny domstolsdatalag. Men denna har fått kritik från Datainspektionen[28] och de användare (i detta fall tingsrätter och kammarrätter)[29] som föreslogs tilldelas större ansvar för IT-system som inte låg under användarnas egen kontroll. Dataskydd.net har också kritiserat den i domstolsdatalagen föreslagna ansvarsfördelningen.[30]

Dålig ansvarsfördelning är en av de huvudsakliga anledningarna till att IT-säkerhet ofta fungerar mindre bra än vad vi önskar. Det finns både starka rättighetsbetonade och ekonomiska skäl för utredarna att tänka om. Sverige bör därför åtminstone överväga att gå samma väg som EU-kommissionen. En ännu modernare inställning vore att som ovan anförs helt avskaffa åtskillnaden mellan personuppgiftsansvariga och personuppgiftsbiträden, då IT-system ändå i dag är så integrerade att det inte i praktiken går att göra någon större åtskillnad mellan dessa olika roller. Dataskydd.net har utvecklat sitt resonemang om risk- och ansvarsfördelning för bättre IT-säkerhet i en rad remissyttranden[31] och artiklar.[32]

Dataskydd.net rekommenderar den nyligen utkomna avhandlingen ”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives” av nederländska säkerhetsforskaren A.M. Arnbak[33] Den redogör på ett begripligt sätt den ekonomiska och juridiska situationen kring IT-säkerhet och ansvarsfördelning i den europeiska lagstiftningen. Sverige är dock inte avvikande från den europeiska normen på något uppenbart sätt, och avhandlingens slutsatser och rekommendationer är giltiga även i den svenska kontexten.

---

[27] Jämför resonemanget om parallella processer kring brott mot marknadsföringslagen och brott mot varumärkeslagen som förs i Bernitz Ulf , Karnell Gunnar , Pehrson Lars , Sandgren Claes. *Immaterialrätt och otillbörlig konkurrens 10de upplagan*. Jure Förlag, 2007.

[28] Datainspektionen: Departementspromemorian Domstolsdatalag (Ds 2013:10). Remissyttrande dnr 361-2013. Tillgänglig på http://www.datainspektionen.se/Documents/remissvar/2013-05-31-domstolsdatalag.pdf

[29] Regeringens proposition 2014/15:148 om en ny domstolsdatalag, s. 32

[30] Dataskydd.net 2015-09-15. Kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag https://dataskydd.net/sites/default/files/domstolsdatalagen_kommentarer_dataskyddnet_ju.pdf

[31] Se https://dataskydd.net/vara-remissvar

[32] I Dagens Juridik – 2015-09-21 *”Omöjligt se efter sina rättigheter – juridisk snårighet och hemlig teknik i nya domstolsdatalagen”*; 2015-10-28 *”Dataskyddet åsidosätts i ny ID-kortslag – lämnar medborgarna maktlösa inför myndigheterna”*

[33] Tillgänglig på http://dare.uva.nl/record/1/492674

Förhållandet till personuppgiftslagen

Personuppgiftslagen bär på många arv från tiden i vilken den uppkom och har på många sätt inte uppnått sina mål. I en studie publicerad av Internetstatistik i februari 2015 framgick att nästan 80% av svaranden på en enkät om dataskydd inte har en god förståelse för hur deras personuppgifter används.[34] Upprepade internationella undersökningar visar att dataskydd och datasäkerhet har en hög prioritet för de tillfrågade.[35] Det finns också en tilltagande känsla av hopplöshet bland privatpersoner – man vill inte få sin integritet kränkt, men ser heller inga realistiska möjligheter att slippa få sin integritet kränkt.[36]

Dataskydd.net föreslår ett starkare och principfastare skydd än det som ges i 9 § personuppgiftslagen (PUL), och tror även att det behövs kraftfullare metoder för privatpersoner att utöva sina rättigheter än de möjligheter som ges i PUL. Bland annat vill Dataskydd.net införa en dataminimeringsprincip. Se mer om detta i kommentarer till kapitel 9.

Dataskydd.net föreslår en omformulering av 8 § PUL, om personuppgiftslagens förhållande till offentlighetsprincipen. Paragrafen bör inte längre inkludera bestämmelser om att myndigheter baserat på historiska och statistiska uppgifter kan fatta beslut om privatpersoner utan att dessa informeras. I kapitel 11 om utlämning av uppgifter kommer Dataskydd.net vidare argumentera för att begränsningen av myndigheters skyldigheter att lämna ut personuppgifter i 2 kap 3 § 3 st Tryckfrihetsförordningen ska göras gällande i de fall då utlämningen av uppgifter resulterar i en otillbörlig påverkan på enskilds möjligheter att utöva sin rätt till privatliv.

Kapitel 9: Avstyrker utredningens förslag om lagens tillämpningsområde

Dataskydd.net avstyrker förslagen om vilka uppgifter som får behandlas. Dataskydd.net avstyrker även förslagen om sökbegränsningar. Dataskydd.net avstyrker förslagen om behandling av särskilda kategorier av uppgifter. I bilaga 1 finns ett tre-kolumns-dokument som sammanställer förslag från utredningen, Dataskydd.net:s ändringsförslag samt kortfattade kommentarer till ändringsförslagen. Brödtexten nedan ger en bredare kontext till Dataskydd.net:s förslag.

Vilka uppgifter får behandlas

Dataskydd.net förordar en ganska annorlunda modell än utredarna vad gäller fastställandet av vilka uppgifter som får behandlas. Medan utredarna har utgått från myndighetens intresse av att uppfylla regeringens krav i myndighetsinstruk-

[34] Delade meningar – Svenska folkets syn på digital integritet 2015.

[35] Se ovan, fotnot 34; Eurobarometer Special Survey 431 ”Data protection”, mars 2015. http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf; CIGI-Ipsos Global Survey on Internet Security and Trust https://www.cigionline.org/internet-survey; Boston Consulting Group ”Data Privacy by the Numbers” https://www.bcgperspectives.com/content/Slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/; Boston Consulting Group, The Value of our Digital Identity, 2013. Tillgänglig på: http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf: Eurobarometer Special Survey 359 ”Attitudes on Data Protection and Electronic Identity in the European Union”, juni 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[36] Turow, Joseph, Hennessey, Michael, Draper, Nora. *The Trade-Off Fallacy – How Marketers are Misrepresenting American Consumers and Openingen Them Up to Exploitation*. Juni 2015. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

tioner, föreskrifter och regleringskrav, vill Dataskydd.net framhålla vikten av att sätta individen i centrum för myndigheternas verksamhet. Detta gäller särskilt då lagens syfte – även i utredarnas förslag – uttryckligen är att ge privatpersoner ett skydd mot kränkning av deras integritet.

En myndighet finns och har ett uppdrag. Uppdraget kan kräva behandling av personuppgifter. Denna behandling måste vara begriplig och transparent för de privatpersoner vars uppgifter behandlas, i förhållande till myndighetens uppdrag.

I stället för att flytta rimlighetsbedömningar till regeringen, riksdagen eller myndigheten själv, bör lagstiftningen utformas på ett sådant sätt att individer bidrar till rimlighetsbedömningarna. De huvudsakliga verktygen för att ge individer en mer aktiv roll i förhållande till myndigheterna vad gäller dataskydd är en samling tydliga principer och tillgång till effektiva rättsmedel för att hävda dessa. Dataskydd.net har framlagt ett antal ändringsförslag som finns i bilaga 1.

Dataskydd.net är alltså av åsikten att det inte krävs ett särskilt regelverk med föreskrifter och förordningar som specifikt tillåter personuppgiftsbehandling, utan tror att personuppgiftsbehandlingen ska ses som en del av verksamheten. Detta stöds av utredningens egna slutsatser, som innefattar att ”den elektroniska förvaltningen är ju inte längre någon särskild del av myndigheternas verksamhet, utan utgör i själva verket förvaltningen” och ”[p]ersonuppgiftsbehandling är en integrerad del i myndigheternas utförande av sina författningsreglerade uppgifter och befogenheter.” Ändamålsbegränsningen som uppstår genom att man definierar myndighetens verksamhet är tillräcklig för att ge en indikation på vilka personuppgifter som ska behandlas. Bättre information till privatpersoner och en möjlighet för privatpersoner att utöva sina rättigheter, till exempel dataminimering, ger privatpersoner möjligheter att agera på och invända mot myndighetens bedömning. Dataskydd.net föreslår att ta bort utredningens föreslagna 31 § myndighetsdatalag.

SOU 2015:39, s. 176

SOU 2015:39, s. 601

Vid ikraftträdandet av en ny myndighetsdatalag kommer myndigheterna alldeles oavsett vilka nya föreskrifter regeringen får utfärda om personuppgifter ha kvar sin gamla praktik. Övergången till en mjukare reglering, där privatpersoner själva ges en aktivare roll i att forma den elektroniska förvaltningen, kan påbörjas från den punkt där myndigheterna befunnit sig innan ikraftträdandet av lagen.

Något om principer. I januari 2012 föreslog EU-kommissionen en dataminimeringsprincip i den nya uppgiftsförordningen, som kodifierades och stärktes av Europaparlamentet i september 2013. Dataminimeringsprincipen innebär att man begränsar insamling, behandling och tillgång till personuppgifter till det absoluta minimum som krävs för att ett visst ändamål ska uppnås. Principen har också stöd hos Datainspektionen[37] och amerikanska nationella institutet för teknisk standardisering (NIST).[38]

KOM(2012)11, Art 5(c)

Europaparlamentet, A7-0402/2013

Dataminimeringsprincipen har stora fördelar ur dataskydds- och datasäkerhetssynpunkt.[39] Det är svårare för myndigheterna att kränka individers

[37] Datainspektionen: Inbyggd integritet. Tillgänglig på http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/

[38] National Institute of Standards and Technology. Special Publication 800-122. ”*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* Tillgänglig på http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[39] Se bl. a. National Institute of Standards and Technology (NIST). Special Publication 800-122. ”*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* Tillgänglig på http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

integritet och privata sfär om uppgiftsinsamlingen är begränsad till det absoluta minimum som krävs för att man ska kunna utföra sina sysslor. Det är också omöjligt att medelst olyckor, säkerhetsfel, slarv eller antagonistiska IT-attacker förlora data man inte samlat in. Både individen och myndigheten blir på det sättet säkrare.

Dataminimering som allmän princip kan således ersätta utredarnas förslag om behandling av personnummer och förslagen om sökbegränsningar.

Förslag till myndighetsdatalag, 11-12 §§

Särskilda kategorier av uppgifter

Dataskydd.net är överens med utredarna om att ”[m]yndigheter bör generellt tillåtas att behandla känsliga personuppgifter som har lämnats i ett ärende eller är nödvändiga för handläggningen av det.” Av detta följer inte att myndigheten utan individens deltagande ska kunna vidta vilka åtgärder som helst. Ändamålsbegränsning, dataminimering, transparens och en möjlighet att effektivt utöva sina rättigheter innebär goda möjligheter för privatpersoner att inte få sin integritet särskilt kränkt även vid behandling av känsliga uppgifter.

SOU 2015:39, s. 306

Det europeiska förbudet mot behandling av särskilt känsliga uppgifter ska dock förstås som en extra skyddsmekanism för privatpersonen mot profilering och särbehandling av privatpersonen på grunder som den inte själv kan råa för.

”Profilering” är ett samlingsbegrepp för åtgärder som stoppar in individer i olika kategorier och grupptillhörigheter beroende på preferenser och individuella förutsättningar. Profilering kan till exempel vara att man behandlas på ett särskilt sätt för att man är kvinna i en viss åldergrupp, eller att man är man av särskild etnisk härkomst med folkbokföringsadress på en viss plats. Åtgärden syftar ofta till att kunna särbehandla individen baserat på dess grupptillhörighet. Det rör sig alltså om positiv eller negativ diskriminering till följd av automatisk databehandling.

Det finns omfattande forskning på diskriminerande effekter av profilering i samband med till exempel marknadsföring,[40] men också ett ökande fokus i forskningen på tillfällen då profilering används för att bevara och befästa rådande normer och stereotyper.[41] Samtidigt finns ett ökande politiskt fokus på profileringstekniker i samband med ”nudging” (knuffning), som innebär att man medelst profilering och belöningar uppmuntrar människor att bete sig på ett sätt som man upplever är bättre för människorna än om de hade fått bete sig

[40] Hildebrandt, Mireille, Gutwirth, Serge (red.). *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Springer Verlag, 2008; Zuiderveen Borgesius, Frederik J., *Improving privacy protection in the area of behavioural targeting*, doktorsavhandling, Universiteit van Amsterdam, 2014; Schrage, Michael. *Big Data's Dangerous New Era of Discrimination*, Harvard Business Review, 29 januari 2014; Bria, Francesca, Clavell, Gemma Galdon, Ruiz, Javier, Zaala, José María, Fitchner, Laura, Halpin, Harry. *D-CENT: Research on digital identity ecosystems*, NESTA, 2015. Tillgänglig på http://www.nesta.org.uk/publications/d-cent-research-digital-identity-ecosystems

[41] Det finns omfattande material om detta, men för ett nyligt exempel på profilering som påverkar arbetssökande kvinnor negativt, se Datta, Amit, Tschantz, Michael Carl, Datta, Anupam. *Automated Experiments on Ad Privacy Settings – A Tale of Opacity, Choice, and Discrimination*. Proceedings on Privacy Enhancing Technologies. Volume 2015, Issue 1, Pages 92–112, ISSN (Online) 2299-0984, DOI: 10.1515/popets-2015-0007, april 2015

som de annars skulle ha gjort.[42]

För viss behandling av känsliga personuppgifter är därför samtyckesprincipen av intresse. Detta gäller till exempel om de känsliga personuppgifterna ska ingå i en samling avsedd för statistisk behandling eller forskning. Det gäller också om de känsliga personuppgifterna ska delas mellan flera myndigheter, vid de tillfällen då privatpersonen kanske själv bara har kännedom om sin relation med en av myndigheterna.

KOM(2012)11, Art 7

Sökbegränsningar

Dataskydd.net menar att utredarnas förslag om sökbegränsningar bottnar i teknisk determinism. Juridiken är inte ett verktyg som kan skydda privatpersonen *trots* tekniken, utan tekniken kan med hjälp av incitament som uppstår ur en väl övervägd juridik designas på ett sådant sätt att privatpersonen skyddas *med hjälp av* tekniken.

Sådan utveckling finns i viss omfattning redan: till exempel investerar myndigheter redan i loggningssystem och accesskontroller. Sådana tekniska lösningar kan användas för att tillgodose utredarnas krav på sökbegränsningar, men de skulle också kunna vara ett transparensverktyg för privatpersoner.

Problemet för varje enskild privatperson är snarare att loggning och accesskontroll görs av myndighetscentrerade säkerhetsbetänkelser snarare än av individcentriska dataskyddsskäl. Om privatpersonerna inte själva bereds tillgång till information om hur deras information och uppgifter behandlas, kan de inte utkräva ansvar av myndigheter som kränker deras integritet.

Dataskydd.net menar att principerna om ändamålsbegränsning, dataminimering och effektiva rättsmedel garanterar den sortens skydd uppdragsgivaren velat uppnå. Om insamling och behandling bara ska ske för särskilda, uttryckliga och berättigade ändamål, och sedan begränsas till minsta möjliga mängd samt inte spridas mer än strikt nödvändigt, är det omöjligt att se hur ett tekniskt system utvecklat för breda sökningar och stor uppgiftsspridning skulle sammanfalla med individens rättigheter. Individer bör emellertid också säkras tillgång till tillräcklig information för att faktiskt kunna utkräva meningsfullt ansvar – man behöver till exempel få veta när saker har gått fel (så som säkerhetsproblem), och när uppgifter ska utlämnas från myndigheter (så att man förstår varifrån påverkan mot den egna personen kan komma), såväl som beredas tillgång till ett påtryckningsmedel (överklagan och ersättning).

De stora utmaningarna för IT-system och dataskydd på myndigheter och i offentlig sektor är inte att de tekniska lösningarna för ett bättre dataskydd inte finns, utan att det finns en inneboende ovilja i stora system mot förändring och förbättring av den egna organisationen och tekniska infrastrukturen. Forskarna Martin Fransson och Johan Quist vid Centrum för tjänsteutveckling vid Karlstads universitet uttrycker det som att ”det är högst osannolikt att medelstilldelning och glada hejarop räcker för att förändra /…/ komplexa system[.]

[42] Återigen finns både generella och specifika exempel, och många studier, men följande exempel på hur man kan manipulera känslotillståndet hos grupper av användare i sociala nätverk är illustrativt: Kramer, Adam D. I. Kramer, Guillory, Jamie E. Guillory, Hancock, Jeffrey T. *Experimental evidence of massive-scale emotional contagion through social networks*. Proceedings of the National Academy of Sciences of the United States of America. Tillgänglig på http://www.pnas.org/content/111/24/8788.full; Alonso, Martin Liby. *Dubbel svensk hemläxa*. DN, 26 juli 2015. Tillgänglig på http://www.dn.se/ledare/signerat/martin-liby-alonso-dubbel-svensk-hemlaxa/

I system som befinner sig i balans kan de bevarande krafterna vara starka. /.../ Vidare att de medel som tilldelats för att förändra systemet, i hög grad gått till att förstärka och befästa det befintliga."[43]

Att ha en alltför preskriptiv lagstiftning som dessutom befäster en redan färdigställd teknisk utveckling, i stället för att lämna öppet för framtida förbättringar när teknologin blir än mer utvecklad, är att skjuta individuella rättigheter i sank. En lättare reglering ger bättre förutsättningar för både professionella IT-arbetare och privatpersoner ("kunder") att ställa krav på hur förvaltningen ska utvecklas, inom ramen för tydligt hållna principer. Dataskydd.net vill mena att en sådan modell dessutom uppmuntrar utveckling och standardisering av teknologier som i ännu högre utsträckning än vad som är fallet i dag hjälper till att garantera de individuella rättigheterna. Se vidare i kommentarerna på kapitel 8 och 10.

Kapitel 10: Avstyrker utredningens förslag om personuppgiftsansvar och säkerhet

Dataskydd.net avstyrker utredningens förslag om personuppgiftsansvar. Dataskydd.net avstyrker också utredningens förslag om säkerhetsåtgärder. I bilaga 1 finns ett tre-kolumns-dokument som sammanställer förslag från utredningen, Dataskydd.net:s ändringsförslag samt kortfattade kommentarer till ändringsförslagen. Brödtexten nedan ger en bredare kontext till Dataskydd.net:s förslag.

Personuppgiftsansvar

Personuppgiftsansvaret är en av många delar i den svenska dataskyddsrätten där den juridiska föreställningen inte motsvarar en teknisk verklighet. Uppdelningen av ansvar mellan personuppgiftsansvariga och personuppgiftsbiträden är förlegad[44,45] och inför EU:s dataskyddsreform riktades kritik mot uppdelningen.[46]

I slutändan finns uppdelningen kvar i EU-kommissionens förslag, men personuppgiftsbiträden ges betydligt större skyldigheter att säkerställa sig om att personuppgiftsansvarig ställer sådana krav att personuppgiftsansvarig kan uppfylla sina förpliktelser. EU-kommissionen har också föreslagit en separat möjlighet att söka skadestånd och utdöma viten mot personuppgiftsbiträden som inte bidrar till att dataskyddslagstiftningens regler upprätthålls.

KOM(2012)11, Art 26(2)(f).

KOM(2012)11, Art 75, 77.

Utredarna föreslår i stället att personuppgiftsbiträden precis som hittills inte ska ges några skyldigheter att vidta sådana åtgärder som hjälper personuppgiftsansvarig att skydda privatpersoners rättigheter. I stället hamnar allt ansvar fortsatt på personuppgiftsansvarig. Utredarna tycks motivera detta med risken för att personuppgiftsansvariga och personuppgiftsbiträden annars skulle skylla på varandra, vilket skulle leda till sämre möjligheter för privatpersonen att

Förslag till myndighetsdatalag, 3 §

Förslag till myndighetsdatalag, 20-21 §§

SOU 2015:39, s. 639

[43] Fransson, M. och J. Quist (2010). Nystartskontoret som blev en tjänst – Om politiska hängrännor i administrativa stuprör (CTF, Karlstad University Studies 2010:39) CTF, Karlstads universitet.

[44] Traung, Peter. *The Proposed New EU General Data Protection Regulation*, Computer Law Review International. Volume 13, Issue 2, Pages 33–49, september 2013

[45] Artikel 29-gruppen. Opinion 3/2010 on the principle of accountability, juli 2010, p. 46. Tillgänglig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

[46] EU-kommissionen, DG Justice, enhet C.3: dataskydd. *Summary of replies to the public consultation about the future legal framework for protecting personal data*. November 2010. Tillgänglig på http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

kräva ersättning vid kränkning. Det är emellertid en juridisk-teknisk invändning, som går att lösa med bättre tillgänglighet till information och ömsesidiga förpliktelser på ansvariga och biträden att hjälpa varandra skydda individens rättigheter, eller en möjlighet att bedriva parallella processer.[47] Även i den nuvarande skadeståndsbestämmelsen i personuppgiftslagen finns en möjlighet för personuppgiftsansvarig att begära jämkning om denne kan påvisa att kränkningen inte var dennes fel. Det vore oönskvärt om ingen kan hållas ansvarig ifall den personuppgiftsansvarige kan hänvisa till ett biträde som, till exempel, inte tillhandahåller någon annan teknisk lösning än den kränkande.

Utredarnas förslag följer regeringens proposition 2014/15:148 om en ny domstolsdatalag. Men denna har fått kritik från Datainspektionen[48] och de användare (i detta fall tingsrätter och kammarrätter)[49] som föreslogs tilldelas större ansvar för IT-system som inte låg under användarnas egen kontroll. Dataskydd.net har också kritiserat den i domstolsdatalagen föreslagna ansvarsfördelningen.[50]

Dålig ansvarsfördelning är en av de huvudsakliga anledningarna till att IT-säkerhet ofta fungerar mindre bra än vad vi önskar. Det finns både starka rättighetsbetonade och ekonomiska skäl för utredarna att tänka om. Sverige bör därför åtminstone överväga att gå samma väg som EU-kommissionen. En ännu modernare inställning vore att som ovan anförs helt avskaffa åtskillnaden mellan personuppgiftsansvariga och personuppgiftsbiträden, då IT-system ändå i dag är så integrerade att det inte i praktiken går att göra någon större åtskillnad mellan dessa olika roller. Dataskydd.net har utvecklat sitt resonemang om risk- och ansvarsfördelning för bättre IT-säkerhet i en rad remissyttranden[51] och artiklar.[52]

Dataskydd.net vill också påpeka att många bestämmelser inte är samma sak som bra bestämmelser. Det finns till exempel inget behov av att påtala att de skyldigheter som en personuppgiftsansvarig ålägger ett personuppgiftsbiträde – även om man upprätthåller skillnaden mellan de båda – ska regleras i ett avtal. Det finns också en risk i att överlägga på personuppgiftsansvarig en allt för omfattande förpliktelse att detaljstyra personuppgiftsbiträdets verksamhet. Ofta överläggs databehandlingen på ett personuppgiftsbiträde just för att personuppgiftsansvarig önskar att begränsa sin egen delaktighet, och därmed också expertis, på databehandling. Risken är överhängande för att avtalen som kommer till stånd under utredningens föreslagna 20-21 §§ inte är tillräckliga för att upprätthålla den nivå av säkerhet som utredarna säkerligen tänkt sig.

Se vidare om detta i kommentarer till kapitel 17.

---

[47] Jämför resonemanget om parallella processer kring brott mot marknadsföringslagen och brott mot varumärkeslagen som förs i Bernitz Ulf , Karnell Gunnar , Pehrson Lars , Sandgren Claes. *Immaterialrätt och otillbörlig konkurrens 10de upplagan*. Jure Förlag, 2007.

[48] Datainspektionen: Departementspromemorian Domstolsdatalag (Ds 2013:10). Remissyttrande dnr 361-2013. Tillgänglig på http://www.datainspektionen.se/Documents/remissvar/2013-05-31-domstolsdatalag.pdf

[49] Regeringens proposition 2014/15:148 om en ny domstolsdatalag, s. 32

[50] Dataskydd.net 2015-09-15. Kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag https://dataskydd.net/sites/default/files/domstolsdatalagen_kommentarer_dataskyddnet_ju.pdf

[51] Se https://dataskydd.net/vara-remissvar

[52] I Dagens Juridik – 2015-09-21 *”Omöjligt se efter sina rättigheter – juridisk snårighet och hemlig teknik i nya domstolsdatalagen”*; 2015-10-28 *”Dataskyddet åsidosätts i ny ID-kortslag – lämnar medborgarna maktlösa inför myndigheterna”*

Säkerhetsåtgärder

Säkerhet är inget statiskt begrepp som alltid innebär samma sak. Avhandlingen ”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives” av nederländska säkerhetsforskaren A.M. Arnbak.[53] redogör på ett begripligt sätt den ekonomiska och juridiska situationen kring IT-säkerhet i den europeiska lagstiftningen. Arnbak gör också en föredömlig genomgång av olika säkerhetsbegrepp. De centrala frågorna är vem som ska hållas säker från vad.

Den europeiska dataskyddsrätten gör det tydligt att det är individen som ska skyddas mot otillbörlig påverkan och kränkning av den egna privata sfären. ”Principerna om inbyggt uppgiftsskydd (data protection by design) och uppgiftsskydd som standard (data protection by default),” är alltså en annan sorts säkerhet än den informationssäkerhet som kodifierats av SIS och som återges av utredningen i avsnitt 10.2.4. Den huvudsakliga skillnaden är att terminologin från Swedish Standard Institute (SIS handbok 550 utgåva 3) inte anger vem som ska gagnas av säkerheten, medan dataskyddslagstiftningen tydligt ställer säkerhet för individen i centrum.

SOU 2015:39, s. 368

SOU 2015:39, s. 375

Det grundläggande problemet – som är välkänt, etablerat och diskuterat i IT-säkerhetsforskningen sedan 1990-talet – är att det saknas anledningar för både företag och myndigheter att investera i bättre IT-säkerhet.[54] Det är helt enkelt billigare och enklare att tillhandahålla osäkra tjänster än att bygga säkra och fungerande tjänster.[55]

Det är för det första svårt för privatpersoner att få reda på när saker går fel. Även om information om säkerhetsbrister rapporteras i medier finns det begränsade möjligheter för privatpersoner att agera på informationen. I svensk dataskyddsrätt saknas till exempel möjlighet att kräva skadestånd från myndigheter som uppenbarligen inte uppfyllt sina förpliktelser att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder.

Redan i början av 1990-talet drogs slutsatsen att starkare konsumenträtt ger mer säkerhet i vanligt använda elektroniska system för samma mängd pengar som annars skulle leda till sämre säkerhet.[56] Forskning stöder att medvetna åtgärder för att ge privatpersoner och konsumenter bättre tillgång till information om säkerhetsproblem i IT-system hjälper dem att utkräva ansvar.[57] Detta gäller särskilt för ansvarsutkrävande i vad man typiskt kan anta vara känsliga system, så som IT-system inom vård och finans.

Privatpersoner är utlämnade till myndigheten för att få reda på vad myndigheten gör. Varje enskild individ kan inte hålla detaljkoll på hur en myndighets datorer fungerar, och privatpersonen är beroende av att myndigheten åläggs informationsplikt så att ansvar kan utkrävas vid rätt tillfälle. Dataskydd.net för-

[53] Tillgänglig på http://dare.uva.nl/record/1/492674

[54] Se den pedagogiska och kortfattade framställningen i introduktionen till Rainer Böhme, ”*Vulnerability Markets – What is the economic value of a zero-day exploit?*” Tillgänglig på https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf

[55] För utförligare kommentarer till detta hänvisar Dataskydd.net till sina remissvar på SOU 2015:23 om en informationssäkerhetsstrategi och SOU 2015:25 om en ny säkerhetsskyddslag. Tillgängliga på: https://dataskydd.net/vara-remissvar

[56] Anderson, Ross. *Why Cryptosystems Fail*. ACM. 1st Conf.- Computer and Comm. Security ’93. Tillgänglig på http://www.cl.cam.ac.uk/users/rja14/wcf.html

[57] Sasha Romanosky, David Hoffman, Alessandro Acquisti *Empirical Analysis of Data Breach Litigation* i WEIS 2010. Tillgänglig på http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf

ordar en individcentrisk incidentrapportering, som ger privatpersonen sådan information som ger dem möjlighet att gå vidare med ansvarsutkrävande. Vi har utvecklat detta i ett remissyttrande på SOU 2015:23 om en svensk informationssäkerhetsstrategi.[58]

I Sverige har möjligheter för individer att själva utöva sina rättigheter hittills mestadels saknats. Tillsynen är i princip begränsad till Datainspektionen, och möjligheten att få skadestånd begränsad. Vad gäller dataskydd är detta särskilt graverande för individen, eftersom de faktorer som ofta förhindrar myndigheter från att göra investeringar i bättre dataskydd coh datasäkerhet är av ekonomisk art. Det finns i princip två saker lagstiftaren kan göra för att ge starkare incitament till myndigheterna att ta dataskydd och datasäkerhet på större allvar. Det ena är att göra bristande förmåga att fokusera på dessa aspekter ekonomiskt kostsamt. Det andra är att se till att privatpersoner får reda på och kan skapa negativ uppmärksamhet för myndigheten kring eftersättande av privatpersonens rättigheter (i princip orsaka ett förtroendetapp för myndigheten om den inte följer lagstiftningen och upprätthåller individuella rättigheter).

De alternativ som utredarna vänder sig till, förslagen i utredningarna om säkerhetsskydd[59] och informationssäkerhetsstrategi,[60] handlar om att låta andra statliga myndigheter (Myndigheten för samhällsskydd och beredskap samt olika polisiära och militära instanser) utöva en sorts granskningsfunktion mot myndigheter som hanterar personuppgifter. SOU 2015:39, s. 381–382

Dessa myndigheter kan för det första inte upprätthålla något dataskydd, eftersom deras uppdrag är formulerat så att de ska skydda samhället, inte individer. Det gör att man kan begränsa diskussionen om deras tillsyn till datasäkerhet.

Myndigheter som föreslås utöva tillsyn i dessa två utredningar har dock en intressekonflikt i det att de samtidigt som de ska bevaka datasäkerhet och statens intresse av att inte drabbas av onödigt stora kostnader. Det finns alltså en risk att de kommer eftersätta i och för sig rimliga organisatoriska och tekniska krav, eftersom deras uppdragsformulering dels kräver att de accepterar statens och myndigheternas organisation sådan som den är (förhoppningsvis är det vedertaget att staten inte ska organisera sig själv och sina myndigheter enligt polisiära och militära direktiv) samt att statens och myndigheternas intressen mycket väl bäst kan tillgodoses av sämre, men billigare, säkerhetsåtgärder.

Kapitel 11: Avstyrker utredningens förslag om utlämning av personuppgifter

Dataskydd.net avstyrker utredningens förslag om direktåtkomst. Dataskydd.net avstyrker också delvis utredningens förslag om annat elektroniskt utlämnande, eftersom de inte garanterar individen eget inflytande och möjlighet till upprättelse vid fel. I bilaga 1 finns ett tre-kolumns-dokument som sammanställer förslag från utredningen, Dataskydd.net:s ändringsförslag samt kortfattade kommentarer till ändringsförslagen. Brödtexten nedan ger en bredare kontext till Dataskydd.net:s förslag.

[58] Se kommentarer på kapitel 9.5 här: https://dataskydd.net/sites/default/files/sou201523_remissyttrande_dataskyddnet.pdf

[59] SOU 2015:25

[60] SOU 2015:23

Dataskydd.net menar att utredarna i viss utsträckning fastnat i teknisk determinism. Tillräckligt förtroende utsträcks inte till att tekniska lösningar går att finna på problem som uppstår då information delas mellan myndigheter. Det leder till en onödigt preskriptiv reglering av specifika utlämningsförfaranden. Andra utlämningsförfaranden lämnas i stort sett oreglerade, då det finns en

> ”presumtion för att ett utlämnande av personuppgifter [från en myndighet] till en annan myndighet inte innebär någon risk för kränkningar av enskildas integritet.”

SOU 2015:39, s. 449

Juridiken är inte ett verktyg som kan skydda privatpersonen *trots* tekniken. Tekniken kan tvärtom genom incitament som uppstår ur en väl övervägd juridik designas på ett sådant sätt att privatpersonen skyddas *med hjälp av* tekniken.

I 31 § PUL och utredningens föreslagna 17 § myndighetsdatalagen står att lämpliga tekniska och organisatoriska åtgärder måste vidtas för att garantera säkerheten vid behandlingen av personuppgifter. Dessa skyldigheter blir också tillämpliga på de oreglerade elektroniska utlämnanden som inte omfattas av utredningens definition av direktåtkomst. Individen får dock inga egna rättigheter och möjligheter att tillse efterlevnaden av dessa bestämmelser, utan upprätthållandet lämnas helt till tillsynsmyndigheten. Tillsynsmyndigheten är dock inget kraftfullare verktyg än att den genom ”påpekanden eller andra åtgärder som inte är tvingande [kan] försöka åstadkomma att myndigheten uppfyller sina skyldigheter enligt denna lag”. En individuell rättighet att få förvänta sig tekniskt och organisatoriskt säkert utlämnande av uppgifter som individen inte själv kan utöva, och som tillsynsmyndigheten inte har mandat att upprätthålla, är i själva verket ingen rättighet.

Föreslagen myndighetsdatalag, 27 §

Det som behövs är tydligare krav på information till privatpersoner om när och hur datadelning mellan myndigheter sker. Denna behöver inkludera

1. Vem som tar del av uppgifter om privatpersonen.
2. Varför uppgifterna ska delas.
3. Hur uppgifterna ska delas.

EU-domstolen har i mål C-201/14[61] uttalat att det inte nödvändigtvis förhåller sig så att enbart lagstöd för en viss sorts datadelning inte innebär tillräcklig information till individer. Domen bör, enligt Dataskydd.net, tolkas så att myndigheterna ges ett aktivt ansvar att berätta för individer hur deras uppgifter sprids mellan olika förvaltningsenheter och på vilket sätt det påverkar dem. Detta ansvar gäller i sin tur oavsett vilken specifik form av utlämnande som sker och hur det har definierats juridiskt.

C-201/14 – Bara m.fl., p. 38

Det kan nämnas att det i utredningsuppdraget står att utredarna ska ”överväga om definitionen av begreppet ”allmän handling” i tryckfrihetsförordningen (TF) är lämpligt utformad när det gäller sådana uppgifter som en myndighet har tillgång till genom s.k. direktåtkomst hos en annan myndighet eller genom liknande former av elektroniskt utlämnande” och ”överväga vilka typer av allmänna handlingar inom de tre verksamhetsområdena som den eller de aktuella myndigheterna ska ha skyldighet att lämna ut elektroniskt och lämna de förslag som dessa överväganden föranleder.” Uppdragsgivaren har också förtydligat att

SOU 2015:39, s. 727

SOU 2015:39, s. 728

[61] Se Curia C-201/14: http://curia.europa.eu/juris/document/document.jsf?text=&docid=168943&pageIndex=0&doclang=SV&mode=lst&dir=&occ=first&part=1&cid=163289

”[e]n upptagning för automatiserad behandling behöver dock aldrig lämnas ut i annan form än utskrift i större utsträckning än vad som följer av lag. Syftet med detta s.k. utskriftsundantag är att förhindra att utlämnade uppgifter behandlas automatiserat på ett sätt som kan medföra otillbörliga integritetsintrång (prop. 1973:33 s. 85 f.).” SOU 2015:39, s. 733

Trots dessa tydliga skrivelser har utredarna i sin behandling av utlämning av uppgifter från myndigheter undvikit problemen med massutlämningar av personuppgifter som sker till aktörer som Lexbase, Ratsit och Birthday. Dessa internetdrivna företag har skapat oro hos tillräckligt många privatpersoner för att Datainspektionen ska ha funnit det nödvändigt med en särskild informationssida om fenomenet.[62] Hemsidornas kartläggning av privatpersoner och deras förehavanden står också i strid mot personuppgiftslagens principer (inte minst bestämmelsen i 21 § PUL om att inga andra än myndigheter ska behandla personuppgifter om lagöverträdelser).

Dataskydd.net understryker att den europeiska dataskyddsrättens ideologiska ramverk, som Sverige har godtagit genom att underteckna Europeiska konventionen för mänskliga rättigheter och genom sitt EU-medlemskap, finns på plats för att privatpersoner ska ges en rimlig möjlighet att utöva inflytande över inte bara vilka de är i dag, utan också vilka de blir. En del av inflytandet är att kunna gå vidare från tidigare misstag.[63]

2 kap 3 § 3 st Tryckfrihetsförordningen lämnar sedan 2002 öppet för att göra bedömningar i lag kring utlämningar av personuppgifter (”[e]n sammanställning av uppgifter ur en upptagning för automatiserad behandling anses dock inte förvarad hos myndigheten om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig.”) som särskilt avser sammanställningar av personuppgifter. I sammanhanget kan också lyftas att allt för vidlyftig tillgång till sammanställningar av personuppgifter (”identitetsinformation”) från myndigheter ökar risken för idenitetsstöld. Det hade egentligen alltså funnits flera anledningar till att utredarna inte borde ha bortsett från denna delen av uppdragsformuleringen. 2 kap 3 § 3 st TF

Kapitel 12: Avstyrker utredningens förslag om överföringar till tredje land

Dataskydd.net avstyrker utredningens förslag om överföringar till tredje land.

Myndigheter behöver inte åberopa ett undantag till personuppgiftslagen för att ”handlägga ärenden med användning av modern teknik genom att kommunicera och kunna förmedla information även till enskilda som befinner sig i avlägsna länder.” Den enskilde har i det här fallet ett eget intresse av att överföringen sker, och kan helt enkelt ge myndigheten sitt samtycke till överföringen. Att överföringar sker från fall till fall på bas av samtycke är överlag mer tillfredsställande än att myndigheterna ges ett brett undantag för allmänt intresse. SOU 2015:39, s. 489-490

Ej heller behöver myndigheterna åberopa undantaget om allmänt intresse för att uppfylla Sveriges internationella förpliktelser. Personuppgiftslagens –

[62] Datainspektionen, Frågor och svar om webbplatser med utgivningsbevis: http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/fragor-och-svar-om-webbplatser-med-utgivningsbevis/

[63] Jämför C-131/12 – Google Spain. Curia: http://curia.europa.eu/juris/liste.jsf?num=C-131/12

och myndighetsdatalagens – bestämmelser är generella och principfasta. De är grundade i flera internationella konventioner. Det går att ifrågasätta om Sverige över huvud taget borde skaffa sig internationella förpliktelser som innebär att principerna inte kan upprätthållas. Man får anta att regeringen, när den underställer sig internationella eller andra mellanstatliga förpliktelser, säkerställer sig om att ”tillräckliga garantier [finns] till skydd för de registrerades rättigheter.”

35 § 1 st personuppgiftslag

Dataskydd.net förordar i stället att 33-35 §§ PUL gäller för överföringar av personuppgifter till tredje land för myndigheter så som de gäller för övriga verksamheter.

Kapitel 13: Avstyrker utredningens förslag om information till den registrerade

Dataskydd.net avstyrker utredningens förslag om information till den registrerade. Vi anser framför allt att det är olyckligt att man fråntar individen möjligheten att ta reda på när en myndighet samlat in information om privatpersonen från någon annan källa än privatpersonen själv. Att ha en särskild lagstiftning som tillämpas bara på personuppgiftsbehandling vid myndigheter borde ses som ett tillfälle att stärka individens rättigheter ännu mer än vad som är fallet i personuppgiftslagen.

I bilaga 1 finns ett tre-kolumns-dokument som sammanställer förslag från utredningen, Dataskydd.net:s ändringsförslag samt kortfattade kommentarer till ändringsförslagen. Brödtexten nedan ger en bredare kontext till Dataskydd.net:s förslag.

Utredarna skriver att de ”inte /…/ nåtts av signaler om att [24 § PUL] inte skulle vara ändamålsenligt utformad eller medföra några särskilda problem för myndigheterna,” och att ”särregler som kommer att behöva meddelas i anslutning till lagen tveklöst torde utgöra bestämmelser av det slag som avses i 24 § andra stycket och som medför undantag från informationsskyldigheten.” Dataskydd.net observerar dock att utredningen inte varit i kontakt med någon organisation som representerar privatpersoner och privatpersoners intressen. Informationsskyldigheten finns heller inte på plats för att minska obehaget för myndigheter, utan för att ge individer en möjlighet till ansvarsutkrävande.

SOU 2015:39, s. 515

SOU 2015:39, s. 516

Dataskydd.net förhåller sig frågande till om man ska undanta vissa typer av eventuella integritetskränkningar (till exempel ”behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning”) från informationsplikten. Dataskydd är ett verktyg genom vilken rätten till privatliv utövas,[64] och bara den omständighet att en viss registrering utgör en minnesanteckning eller ej färdigställd handling behöver inte innebära att den inte är eller kan vara integritetskränkande.

Föreslagen myndighetsdatalag, 23 §

Myndigheter och andra personuppgiftsansvariga ges redan breda möjligheter att inte lämna ut information om det skulle vara för betungande att göra det. Myndigheten väljer själv vad som är betungande och för flera instanser gäller att bedömningen inte går att överklaga (jämför utredningens förslag till 33 § myndighetsdatalag). Det känns inte övertygande att utredarna föreslår att skapa ett särskilt undantag från informationsplikten som även täcker tillfällen då det

[64] Se ovan, fotnot 5

förvisso inte är betungande men upplevs som jobbigt av andra skäl att lämna ut uppgifterna av andra skäl.

Snarare än att utreda hur myndigheterna kan stärkas i sina befogenheter att värja sig mot de mekanismer som står privatpersoner till buds för att utkräva ansvar borde utredarna ha styrkt individens rättigheter.

Dataskydd.net är i övrigt tillfredsställda att 12 kap. 1 § OSL garanterar att undantaget för myndigheter från informationsskyldighet vid sekretess bara i undantagsfall kan göras gällande.

SOU 2015:39, s. 496

Kapitel 14: Avstyrker utredningens förslag om arkivering och gallring

Vad gäller gallring och arkivering bör principen vara att personuppgifter inte ska behandlas längre än vad som är strikt nödvändigt för att utföra uppdraget (ändamålsbegränsning och dataminimering). Att man inte lagrar personuppgifter betyder inte att det inte går att dokumentera myndighetens verksamhet. Dataskydd.net anser att man huvudsakligen inte ska arkivera direkta personuppgifter, utan begränsa arkiveringsfunktionen till mindre genomtränglig information så som initialer (det vill säga, i praktiken en sorts pseudonymisering av de berörda individerna).

Europaparlamentet, A7-0402/2013 Art 2(a): pseudonymiserade uppgifter: personuppgifter som inte kan hänföras till en specifik registrerad utan att kompletterande uppgifter används, så länge dessa hålls separata och är underkastade tekniska och organisatoriska åtgärder för att garantera att inget sådant hänförande är möjligt.

En väl fungerande ändamålsbegränsning och dataminimering är förvisso tillräckligt för att arkiverad information inte ska bli graverande för individer på lång sikt. Jämför emellertid också ett nytt rättsfall från Italien, som anvisats till EU-domstolen angående den så kallade ”rätten att bli bortglömd”. Fallet berör precis när myndigheter - och företag som agerar biträden åt myndigheter - kan komma att omfattas av en skyldighet att göra information mer svårtillgänglig.[65] Istället för att hamna i den olyckliga situationen att EU-rätten begränsar viktiga insynsfunktioner i svensk offentlig förvaltning, borde man så snart som möjligt agera för bästa möjliga transparens i förvaltningen till minsta möjliga ”dataskyddskostnad” för individen.

C-398/15 – Manni

Kapitel 15: Avstyrker utredningens förslag om skyldigheter att vidta åtgärder då behandling av personuppgifter är oriktig eller otillåten

Dataskydd.net finner det lovvärt att man vill ge individen möjligheter att ställa saker till rätta som varit fel, men är inte överens med utredarna om att denna möjlighet ska vara svagare i myndighetsdatalagen än vad den är i personuppgiftslagen. Utredningens förslag är också mycket svagare än den möjlighet att ställa felaktigheter till rätta som föreslås i EU:s dataskyddsförordning.

Dataskydd.net förordar istället direkt tillämplighet av 28 § PUL. Utredningen konstaterar att frågan om rättelse ändå ofta reglerats genom en hänvisning till 28 § personuppgiftslagen i de särskilda registerförfattningarna, så det borde inte innebära någon större skillnad mot idag. Eftersom brottsbekämpande verksamhet inte täcks av den föreslagna myndighetsdatalagen, finns ingen anledning att tro att de särskilda undantag som listas i 8a § PUL skulle göras gällande och undergräva individers rättigheter enligt 28 § PUL.

SOU 2015:39, s. 556

SOU 2015:39, s. 553

[65] Läs mer: https://jefausloos.wordpress.com/2015/09/18/cjeu-is-asked-to-rule-on-the-right-to-be-forgotten-again/

Kapitel 16: Stödjer utredningens förslag om anmälan till tillsynsmyndigheten m.m.

Dataskydd.net stödjer utredningens förslag om förteckningar. Dataskydd.net vill dock understryka att en förteckning som sådan inte är hjälpsam för privatpersoner annat än om den innehåller sådan information som hjälper privatpersonen etablera att handlingen av personuppgifter hos myndigheten sker i enlighet med lagens bestämmelser i övrigt.

Dataskydd.net hade föredragit om utredningen begränsat skyldigheten att utse personuppgiftsombud efter hur många uppgifter som behandlas, snarare än genom att undanta samtliga myndigheter från förpliktelsen att utse personuppgiftsombud. Dataskydd.net hade också föredragit om förteckningarna specificerades bli utformade på ett sådant sätt att effektivt ansvarsutkrävande av myndigheter med avseende på deras uppfyllande av dataskyddsförpliktelser förenklas. Se även ovan, avsnittet om säkerhetsåtgärder i kommentarerna till kapitel 10.

Kapitel 17: Avstyrker delvis utredningens förslag om tillsynsmyndighetens befogenheter

Dataskydd.net avstyrker delvis utredningens förslag om tillsynsmyndighetens befogenheter. Som Dataskydd.net motiverar ovan finns dock ett behov av effektiva rättsmedel för enskilda att använda sig av när de fått reda på att myndigheter inte behandlat deras uppgifter i enlighet med lagen.

Utredarna föreslår i stället att personuppgiftsbiträden precis som hittills inte ska ges några skyldigheter att vidta sådana åtgärder som hjälper personuppgiftsansvarig att skydda privatpersoners rättigheter. I stället hamnar allt ansvar fortsatt på personuppgiftsansvarig. Utredarna tycks motivera detta med risken för att personuppgiftsansvariga och personuppgiftsbiträden annars skulle skylla på varandra, vilket skulle leda till sämre möjligheter för privatpersonen att kräva ersättning vid kränkning. Det är emellertid en juridisk-teknisk invändning, som går att lösa med bättre tillgänglighet till information och ömsesidiga förpliktelser på ansvariga och biträden att hjälpa varandra skydda individens rättigheter, eller en möjlighet att bedriva parallella processer.[66] Även i den nuvarande skadeståndsbestämmelsen i personuppgiftslagen finns en möjlighet för personuppgiftsansvarig att begära jämkning om denne kan påvisa att kränkningen inte var dennes fel. Det vore oönskvärt om ingen kan hållas ansvarig ifall den personuppgiftsansvarige kan hänvisa till ett biträde som, till exempel, inte tillhandahåller någon annan teknisk lösning än den kränkande.

Förslag till myndighetsdatalag, 3 §

Förslag till myndighetsdatalag, 20-21 §§

SOU 2015:39, s. 639

Möjligheten att utkräva ansvar på rätt plats i den tekniska näringskedjan är direkt korrelerad med möjligheterna att få ett starkt dataskydd och en god datasäkerhet.

I Sverige har möjligheter för individer att själva utöva sina rättigheter hittills varit ganska få. Tillsynen är i princip begränsad till Datainspektionen, och möjligheten att få skadestånd begränsad. Vad gäller dataskydd är detta särskilt graverande för individen, eftersom de faktorer som ofta förhindrar myndigheter

[66] Jämför resonemanget om parallella processer kring brott mot marknadsföringslagen och brott mot varumärkeslagen som förs i Bernitz Ulf , Karnell Gunnar , Pehrson Lars , Sandgren Claes. *Immaterialrätt och otillbörlig konkurrens 10de upplagan*. Jure Förlag, 2007.

från att göra investeringar i bättre dataskydd coh datasäkerhet är av ekonomisk art. Det finns i princip två saker lagstiftaren kan göra för att ge starkare incitament till myndigheterna att ta dataskydd och datasäkerhet på större allvar. Det ena är att göra bristande förmåga att fokusera på dessa aspekter ekonomiskt kostsamt. Det andra är att se till att privatpersoner får reda på och kan skapa negativ uppmärksamhet för myndigheten kring eftersättande av privatpersonens rättigheter (i princip orsaka ett förtroendetapp för myndigheten om den inte följer lagstiftningen och upprätthåller individuella rättigheter).

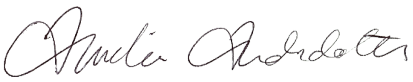
En möjlighet till skälig ersättning för den skada och kränkning som uppstått bör införas, tillsammans med breda möjligheter för den enskilde att själv gå till handling vid de tillfällen tillsynsmyndigheten av resursskäl kanske tvingas prioritera annorlunda.

Dataskydd.net avstyrker förslaget att omfattningen i vilken privatpersoner ska kunna överklaga beslut enligt lagen begränsas. Dataskydd är privatpersonernas verktyg för att skydda och utöva sin rätt till privatliv. Lagskyddet måste vara robust, och tillhandahålla effektiva och meningsfulla sätt för privatpersonen att använda verktyget.

Slutligen vill Dataskydd.net föra upp möjligheten att utsträcka till Datainspektionen en ombudsmannafunktion, liknande den som finns hos Diskrimineringsombudsmannen. För att privatpersoner ska ha goda förutsättningar att skydda sina personuppgifter kan de behöva råd och stöd från en ombudsperson. Ombudspersonen, men också andra organisationer, bör kunna föra enskildas talan å deras vägnar i domstol i frågor som rör dataskydd. Funktionen ”dataombudsman” föreslogs på 1970-talet,[67] men avfärdades då, och återuppstod bara i form av ”dataansvariga” i slutet av 1980-talet.[68] En ”dataansvarig” tillhör dock den felande verksamheten, och om en genuin intressekonflikt uppstår mellan verksamheten och privatpersonen (se ovan) är det svårt att se att en ansvarig från verksamheten inte främst skulle ta verksamhetens eget parti.

Frågan om dataombudsmän är nu emellertid uppe till prövning i EU-domstolen, genom C-192/15 – Rease.[69] Eftersom rätten till dataskydd och rätten till privatliv är individuella rättigheter, är frågan till EU-domstolen om dataskyddsmyndigheter alls har en rättighet att kategoriskt avfärda utredning av omständigheter som bara drabbat en enskild eller ett fåtal enskilda. Oavsett det europeiska utfallet är det inte dåligt om Sverige förstärker individers möjligheter att utöva sina rättigheter genom införandet av en ombudsmannafunktion.

C-192/15 – Rease



Amelia Andersdotter
Ordförande, Dataskydd.net

[67] SOU 1972:47 Data och integritet, kapitel 10

[68] SOU 1986: 24, Integritetsskyddet i informations samhället 1 (Rättelse och skadestånd/Patientuppgifter i personregister), kapitel 4.7

[69] EULawRadar. *Case C-192/15, Rease – secretly spied on, medical data leaked, and left unprotected by the Dutch regulator*. Se http://eulawradar.com/case-c-19215-rease-secretly-spied-on-medical-data-leaked-and-left-unprotected-by-the-dutch-regulator/

BILAGA 1: Sammanställda ändringsförslag

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
1 § Syftet med denna lag är att ge myndigheter möjligheter att behandla personuppgifter på ett ändamålsenligt sätt i deras verksamheter och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.	1 § Syftet med denna lag är att ge är att ge myndigheter möjligheter att behandla personuppgifter på ett ändamålsenligt sätt i deras verksamheter och att ge privatpersoner tillräckliga verktyg att utöva deras grundläggande rätt till dataskydd och privatliv, samt personliga integritet i förhållande till verksamheten.	Rättighetskatalogen hamnar på detta vis närmare den rättighetskatalog som återfinns i de internationella konventioner och stadgor som Sverige är bundet av. Ändringen har också till syfte att förtydliga att individer kan ges en aktiv roll i upprätthållandet av sina egna rättigheter, vilket överensstämmer väl med den bild av en aktiv privatperson som ofta förekommer i samband med visioner om en elektronisk (och framför allt internettillgänglig) förvaltning.	s. 9-10
2 § Denna lag gäller vid myndigheters behandling av personuppgifter. Lagen gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.	(INGEN ÄNDRING)	—	—
3 § Lagen ska inte tillämpas vid behandling av personuppgifter i 1. en myndighets administrativa verksamhet, 2. en myndighets verksamhet som personuppgiftsbiträde, eller 3. den verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder.	3 § Lagen ska inte tillämpas vid behandling av personuppgifter i den verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder. Lagen skall inte heller tillämpas vid administration av myndighetens anställda.	Åtskillnaden mellan personuppgiftsbiträden och personuppgiftsansvariga tas bort, vilket förtydligar omständigheten att alla myndigheter har lika skyldigheter att säkerställa människors möjligheter att förebygga att och utkräva ansvar då deras grundläggande rätt till dataskydd och privatliv, samt deras personliga integritet, påverkas av sådan behandling på ett otillbörligt sätt. Undantaget för administrativ verksamhet förtydligas genom att klargöra att detta åsyftar behandling av personuppgifter som rör myndighetens verksamhet som arbetsgivare, snarare än dess verksamhet som myndighetsutövare.	s. 10-11
4 § Om det i en annan lag eller förordning än som avses i 5 § finns bestämmelser som avviker från denna lag, ska de bestämmelserna gälla.	(UTGÅR)	Enskilda ska inte behöva ägna sina liv åt att läsa författningar för att få en begriplig översikt över sina rättigheter.	s. 13

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
5 § Om inte annat anges i 6 § gäller denna lag i stället för personuppgiftslagen (1998:204) eller föreskrifter som meddelats i anslutning till den lagen.	5 § Definitioner, begrepp och förpliktelser enligt denna lag ska vara samma som i personuppgiftslagen (1998:204), så länge denna lag inte anger annorlunda förpliktelser än som där förekommer.	Specialreglering av myndigheter bör syfta till att ge individen starkare rättigheter än vad de har i personuppgiftslagen.	s. 11-12
6 § Följande bestämmelser i personuppgiftslagen (1998:204) ska tillämpas på motsvarande sätt när personuppgifter behandlas enligt denna lag eller föreskrifter som meddelats med stöd av den: 1. 3 § om definitioner, 2. 8 § om förhållandet till offentlighetsprincipen m.m., 3. 9 § om grundläggande krav på behandlingen, 4. 13, 15, 16, 18 och 19 §§ om känsliga personuppgifter, 5. 23 och 25 §§ om information till den registrerade som ska lämnas självmant, 6. 26 § om information till den registrerade som ska lämnas efter ansökan, 7. 33–35 §§ om överföring av personuppgifter till tredjeland, 8. 38 och 40 §§ om personuppgiftsombud, och 9. 48 § om skadestånd. I 23 § finns bestämmelser om undantag från informationsskyldigheten enligt första stycket 5 och 6.	6 § Följande bestämmelser i personuppgiftslagen (1998:204) ska tillämpas på motsvarande sätt när personuppgifter behandlas enligt denna lag eller föreskrifter som meddelats med stöd av den: 1. 3 § om definitioner, 2. 13, 15, 16 och 18 §§ om känsliga personuppgifter, 3. 23-25 §§ om information till den registrerade som ska lämnas självmant, 4. 26 § om information till den registrerade som ska lämnas efter ansökan, 5. 28 § om rättelse, 6. 29 § om automatiserade beslut, 7. 33–35 §§ om överföring av personuppgifter till tredjeland, och 8. 38 och 40 §§ om personuppgiftsombud. I 23 § finns bestämmelser om undantag från informationsskyldigheten enligt första stycket 4 och 5.	Se kommentarer ovan i kommentarer till kapitel 8.	s. 11-12

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
	6 a § Behandling av personuppgifter ska äga rum enligt följande principer: 1. behandlingen ska ske på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet) 2. insamling och behandling ska ske för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning). 3. insamling av uppgifter ska vara begränsad till minsta möjliga mängd för att uppfylla syftet för vilka uppgifterna behandlas; behandling av uppgifter ska vara relevant för syftet, ska inte innebära större spridning av uppgifterna än strikt nödvändigt, och fortgå bara så länge som syftena inte kan uppnås genom att man behandlar information som inte rör personuppgifter (dataminimering). 4. De ska vara riktiga och när så är nödvändigt aktuella; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är oriktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (riktighet). 5. De ska behandlas på ett sätt som ger de registrerade möjlighet att effektivt utöva sina rättigheter (effektivitet). Tillsynsmyndigheten får utfärda föreskrifter om närmare precision av var och en av dessa principiella hållningspunkter. Förhållandet till offentlighetsprincipen anges i 6 b § och 15 §. Behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål återfinns i 6 c §.	Listan med principer är hämtad från Europaparlamentets ändringsförslag till EU-kommissionens dataskyddsförordning. Krav 2, 3 och 5 i samverkan ger principiellt starka verktyg för individer att själva delta i upprätthållandet av sina rättigheter. De allmänna principerna kommer dock att behöva kompletteras med ytterligare informationsplikt som förtydligas i kommentarerna till kapitel 10.	s. 12-14
	6 b § Bestämmelserna i denna lag tillämpas inte i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Bestämmelserna hindrar inte heller att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.	Bestämmelser om att myndigheter baserat på historiska och statistiska uppgifter kan fatta beslut om privatpersoner utan att dessa informeras och kan invända syftar inte till att låta folket granska makten, utan till att låta makten granska folket. Dataskydd uppstod som rättighet bland annat för att motverka sådan motvänd granskning.	s. 12, 20-21
	6 c § Behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål skall anses som förenlig med de ändamål för vilka uppgifterna samlades in enligt 6 a § 2, om samhällsintresset av detta nya ändamål klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. Reglerna i 17 § denna lag och 23-26 och 28 §§ personuppgiftslagen ska fortfarande vara tillämpliga.	—	s. 12-14

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
7 § En myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Personuppgiftsansvaret enligt första stycket omfattar även behandling som en myndighet utför genom direktåtkomst till personuppgifter hos en annan myndighet eller enskild.	7 § Den myndighet är personuppgiftsansvarig för behandling av personuppgifter som haft kontakt med privatpersonen och från privatpersonen insamlat personuppgifterna. Privatpersonen ska informeras om personuppgiftsbiträden och biträden som anlitats av ett personuppgiftsbiträde. Om uppgifter utlämnas till andra myndigheter, ska syftet med utlämningen delges privatpersonen på förhand. Privatpersonen ska också beredas möjlighet att ta ställning till utlämningen.	Dataskydd.net inte ser behovet av en fortsatt åtskillnad mellan personuppgiftsbiträden och personuppgiftsansvariga vad gäller ansvaret för dataskydd gentemot privatpersonen. Respekt för den enskilde behöver genomsyra hela den tekniska och organisatoriska näringskedjan.	s. 16-17
8 § Personuppgifter får behandlas om det är nödvändigt för att en myndighet ska kunna utföra sin verksamhet.	8 § Personuppgifter får behandlas enligt principerna i 6 § för att en myndighet ska kunna utföra sin verksamhet.	Myndigheterna får utföra sitt uppdrag, och genom 6 § ges privatpersoner en aktivare roll i att samverka med myndigheten kring vad detta betyder i relation till deras dataskydd och privatliv.	s. 12-14
9 § Behandling som är tillåten enligt denna lag eller föreskrifter som meddelats med stöd av den får utföras även om den registrerade motsätter sig behandlingen.	(UTGÅR)	Det behövs inget ytterligare klargörande att individen i allmänhet inte har en rätt att samtycka till behandling enligt denna lag. Det framgår redan av att myndigheterna får rätten att genomföra sitt uppdrag i 8 §.	s. 12-14
10 § Utöver vad som följer av 15, 16, 18 och 19 §§ personuppgiftslagen (1998:204) får känsliga personuppgifter behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av det eller om uppgifterna behandlas endast i löpande text.	10 § Utöver vad som följer av 15, 16, och 18 §§ personuppgiftslagen (1998:204) får känsliga personuppgifter behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av det eller om uppgifterna behandlas endast i löpande text. 19 § personuppgiftslagen är inte tillämplig på känsliga personuppgifter som lämnats in eller inhämtats till följd av myndighetsutövning.	Dataskydd.net är kritiska till att känsliga personuppgifter som samlats in genom myndighetsutövning ska kunna lämnas ut till forskningsändamål utan individens föregående samtycke.	s. 14
11 § Personnummer eller samordningsnummer får tas in i ett beslut endast om beslutet rör en enskilds identitet eller motsvarande personliga förhållanden, det är nödvändigt för att beslutet ska kunna verkställas eller det krävs med hänsyn till beslutande myndighets behov av identifieringsuppgifter.	(UTGÅR)	Det behövs ingen specifik reglering av person- och samordningsnummer, om ändamålsbegränsningen, dataminimeringen, transparensen och det effektiva utövandet av rättigheterna i Dataskydd.net:s föreslagna 6 § upprätthålls.	s. 12-14

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
12 § Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackföreening liksom uppgifter som rör hälsa eller sexualliv får användas som sökbegrepp endast om det är tillåtet enligt föreskrifter som tagits in i bilaga till denna lag eller i annan lag eller förordning. Vad som sägs i första stycket gäller inte vid en sökning i en viss handling eller i ett visst ärende.	(UTGÅR)	Det behövs ingen specifik reglering av tillgångsbegränsning för enskilda tjänstemän, om ändamålsbegränsningen, dataminimeringen, transparensen och det effektiva utövandet av rättigheterna i Dataskydd.net:s föreslagna 6 § upprätthålls.	s. 15
13 § Direktåtkomst till personuppgifter som är sekretessreglerade är tillåten endast i den utsträckning som anges i bilaga till denna lag eller i annan lag eller förordning. Med sekretessreglerade uppgifter avses detsamma som i offentlighets- och sekretesslagen (2009:400). Vad som sägs i första stycket gäller inte direktåtkomst som medges 1. den registrerade eller dennes ombud till uppgifter som hänför sig till den registrerade, 2. till personuppgifter som är sekretessreglerade enligt 21 kap. 7 § offentlighets- och sekretesslagen, 3. ett personuppgiftsbiträde, eller 4. en myndighet endast för sådan teknisk bearbetning eller teknisk lagring som avses i 2 kap. 10 § första stycket tryckfrihetsförordningen för den utlämnande myndighetens räkning.	(UTGÅR)	Dataskydd.net:s förslag på ändringar i 7 § är mer teknikneutrala och sätter individens möjlighet att få tillräcklig information för att själv utkräva ansvar i centrum.	s. 19-21
14 § Innan en myndighet medger direktåtkomst till personuppgifter ska myndigheten göra en risk- och sårbarhetsanalys och komma överens med mottagaren av personuppgifterna hur skyddet för personuppgifterna ska säkerställas. Av överenskommelsen ska också framgå hur utövandet av de skyldigheter som personuppgiftsansvaret innefattar ska ske. Vad som sägs i första stycket ska i tillämpliga delar även gälla då en myndighet på annat sätt än genom direktåtkomst samarbetar med andra myndigheter eller enskilda på sätt som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem.	(UTGÅR)	Dataskydd.net:s förslag på ändringar i 3 och 7 §§ är mer teknikneutrala och sätter individens möjlighet att få tillräcklig information för att själv utkräva ansvar i centrum.	s. 19-21

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
15 § Får en personuppgift lämnas ut till en enskild, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften.	15 § Får en personuppgift lämnas ut, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften, och så länge utlämnandet inte resulterar i en otillbörlig påverkan på enskilds möjligheter att utöva sina rätt till privatliv.	Dataskydd.net ämnar med detta tillägg åtgärda öppen och aggressiv kartläggning av privatpersoners livsbetingelser. Paragrafen är kopplad till rätten till privatliv, snarare än rätten till dataskydd, för att ge luftigare tolkningsutrymme till påverkansbegreppet.	s. 12, 20-21
16 § Utöver vad som följer av 34 § personuppgiftslagen (1998:204) eller av föreskrifter eller beslut som meddelats med stöd av 35 § samma lag får personuppgifter överföras till tredjeland som saknar adekvat skyddsnivå, om 1. överföringen krävs för handläggningen av ett visst ärende, eller 2. överföringen är nödvändig för att fullgöra en uppgiftsskyldighet som följer av lag eller förordning eller avtal med annan stat eller mellanfolklig organisation som Sverige har tillträtt eller annars är förpliktat att följa.	(UTGÅR)	Samtycke är en tillräcklig bas för att individer som vill ha hjälp av myndigheter ska få det, även om de befinner sig i tredje land. Sverige borde inte skaffa sig internationella förpliktelser som innebär att dataskyddsprinciperna inte kan upprätthållas, men även om Sverige gjorde det så skulle de inhemska reglerna i sådana fall ställas åt sidan genom hänvisningen till personuppgiftslagens bestämmelser i Dataskydd.net:s föreslagna 5 §.	s. 21
17 § En myndighet ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder samt åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och karaktären hos de uppgifter som ska skyddas. Vid utformningen av säkerhetsåtgärderna ska myndigheten även beakta bestämmelser om informationssäkerhet i annan författning som gäller för myndigheten.	17 § En myndighet ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder samt åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och karaktären hos de uppgifter som ska skyddas. I de fall då de tekniska och organisatoriska åtgärderna inte fortlöper som förutsett, ska privatpersoner som berörs av störningen informeras om hur deras uppgifter berörs och vad de kan göra för att skydda sig mot negativa konsekvenser av störningen. Om störningen berott på tekniska eller organisatoriska problem på myndigheten ska privatpersonen ha rätt till skälig ersättning för kränkningen som uppstått därav. Informationen till privatpersoner om störningen ska vara tillräcklig för att privatpersonen ska kunna göra en bedömning om huruvida den är ersättningsberättigad. Vid utformningen av säkerhetsåtgärderna ska myndigheten även beakta bestämmelser om informationssäkerhet i annan författning som gäller för myndigheten.	Dataskydd.net har tidigare lyft vikten av individcentrisk incidentrapportering. Det finns starka indikationer på att sådan rapportering förbättrar IT-säkerhet, givet att rapporteringssystemet utformas på ett sådant sätt att individer kan använda incidentrapporterna för effektivt ansvarsutkrävande när detta är motiverat.	s. 17-19

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
18 § Tillgången till personuppgifter ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.	(UTGÅR)	Det behövs ingen specifik reglering av tillgångsbegränsning för enskilda tjänstemän, om ändamålsbegränsningen, dataminimeringen, transparensen och det effektiva utövandet av rättigheterna i Dataskydd.net:s föreslagna 6 § upprätthålls.	s. 12-15
19 § Ett personuppgiftsbiträde eller den som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Detta gäller även för biträden som anlitats av ett personuppgiftsbiträde. Personuppgiftsbiträden och underbiträden har att vissa samma aktsamhet för privatpersonens möjlighet att effektivt utöva sina rättigheter enligt lagen som personuppgiftsansvariga.	19 § Ett personuppgiftsbiträde eller den som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Detta gäller även för biträden som anlitats av ett personuppgiftsbiträde. Personuppgiftsbiträden och underbiträden har att vissa samma aktsamhet för privatpersonens möjlighet att effektivt utöva sina rättigheter enligt lagen som personuppgiftsansvariga.	Dataskydd.net inte ser behovet av en fortsatt åtskillnad mellan personuppgiftsbiträden och personuppgiftsansvariga vad gäller ansvaret för dataskydd gentemot privatpersonen. Respekt för den enskilde behöver genomsyra hela den tekniska och organisatoriska näringskedjan.	s. 16-17, 23-24
20 § När en myndighet anlitar ett personuppgiftsbiträde, ska myndigheten förvissa sig om att biträdet 1. ser till att personuppgifter behandlas bara i enlighet med instruktioner från myndigheten, 2. kan genomföra de säkerhetsåtgärder som avses i 17 § och som måste vidtas till skydd för de personuppgifter som biträdet behandlar, 3. fortlöpande vidtar säkerhetsåtgärderna, och 4. inte anlitar annat biträde utan godkännande från myndigheten.	(UTGÅR)	Dataskydd.net ser inget behov av att ha kvar dessa bestämmelser. Dels följer bestämmelsen redan av 19 §. Dels är en modernare ansvarsfördelning för dataskyddet mellan de olika aktörerna så som föreslagen i Dataskydd.net:s 7 § bättre för att uppnå de önskade skyddsnivåerna.	s. 16-17, 23-24
21 § Det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för myndighetens räkning. Avtalet ska innehålla instruktioner och villkor om personuppgiftsbiträdets skyldigheter i frågor som avses i 19 och 20 §§. Motsvarande avtal ska finnas med ett biträde som anlitats av ett personuppgiftsbiträde.	(UTGÅR)	__ ”__	s. 16-17, 23-24

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
22 § En myndighet ska föra en förteckning över de behandlingar som myndigheten utför med stöd av denna lag. Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.	(INGEN ÄNDRING)	—	—
23 § Bestämmelserna i 23, 25 och 26 §§ personuppgiftslagen (1998:204) ska inte tillämpas i den utsträckning som en uppgift inte får lämnas ut till den registrerade på grund av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller föreskrifter som meddelats med stöd av den lagen. Bestämmelserna i 26 § personuppgiftslagen behöver inte tillämpas vid behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter.	23 § Bestämmelserna i 23, 24, 25 och 26 §§ personuppgiftslagen (1998:204) ska inte tillämpas i den utsträckning som en uppgift inte får lämnas ut till den registrerade på grund av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller föreskrifter som meddelats med stöd av den lagen.	Undantaget för sekretess utsträcks till förpliktelserna i 24 § (som blivit gällande på grund av föreslagna ändringar i 5 §), och det särskilda undantaget från 26 § vid ej sökbara personuppgiftssamlingar tas bort.	s. 21-22
24 § En personuppgift ska på begäran av den registrerade rättas eller kompletteras om uppgiften rör honom eller henne och den är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i myndighetens eller någon annans bedömning.	(UTGÅR)	Det framstår som omotiverat att avlasta myndigheter från skyldighet att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med denna lag, och därmed försvaga individens ställning. Myndigheter och allmänheten i övrigt tjänar inte på att felaktig och ofullständig information blir kvar. För individer kan undlåtande att avhjälpa felet leda till problem.	s. 22-23
25 § En personuppgift ska på begäran av den registrerade avskiljas från fortsatt behandling och inte lämnas ut till en enskild annat än med stöd av 2 kap. tryckfrihetsförordningen eller utplånas, om uppgiften rör honom eller henne och den inte får behandlas enligt denna lag. Vad som sägs i första stycket gäller inte personuppgifter i ett beslut.	(UTGÅR)	__ ”__	s. 22-23

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
	25 a § En privatperson har rätt till skälig ersättning för den skada och kränkning som uppstått i de fall då en myndighet inte behandlat dess personuppgifter så som föreskrivs i denna lag. Vidare ska skälig ersättning utgå ifall säkerhetsåtgärder enligt 17 § inte fortlöpt som förutsett på grund av omständigheter myndigheten rimligtvis kunnat undvika.	Bestämmelsen kan behöva kompletteras ytterligare enligt förhållanden beskrivna i kommentarer på kapitel 17.	s. 23-24
	25 b § Tillsynsmyndigheten ska genom råd och på annat sätt medverka till att den som utsatts för diskriminering kan ta till vara sina rättigheter.	Saxat från 2 § lagen om diskrimineringsombudsmannen (2008:568). Dataskydd.net anser det rimligt att privatpersoner ges rätt och stöd att utöva sina rättigheter enligt lagen.	s. 23-24
	25 c § Tillsynsmyndigheten, eller en ideell förening, får som part föra talan för en enskild som medger det. När ombudsmannen eller föreningen för sådan talan får ombudsmannen eller föreningen i samma rättegång också föra annan talan för den enskilde om han eller hon medger det.	Saxat från 6 kap 2 § diskrimineringslag (2008:567). Dataskydd.net anser det rimligt att privatpersoner ges rätt och stöd att utöva sina rättigheter enligt lagen.	s. 23-24
26 § Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få 1. tillgång till de personuppgifter som behandlas, 2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och 3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.	(INGEN ÄNDRING)	—	—
27 § Om tillsynsmyndigheten konstaterar att en myndighet kan komma att behandla personuppgifter på ett olagligt sätt, ska tillsynsmyndigheten genom påpekanden eller andra åtgärder som inte är tvingande försöka åstadkomma att myndigheten uppfyller sina skyldigheter enligt denna lag eller föreskrifter som meddelats med stöd av den.	27 § Om tillsynsmyndigheten konstaterar att en myndighet kan komma att behandla personuppgifter på ett olagligt sätt, ska tillsynsmyndigheten genom påpekanden eller andra åtgärder som inte är tvingande (till exempel informationsutskick till berörda privatpersoner) försöka åstadkomma att myndigheten uppfyller sina skyldigheter enligt denna lag eller föreskrifter som meddelats med stöd av den.	Om det finns en risk att privatpersonernas rättigheter kan komma att kränkas, är det rimligt att de ges en möjlighet att själva utvärdera och bidra i den beslutsprocess som leder dit.	s. 23-24

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
28 § Tillsynsmyndigheten får förelägga en myndighet att uppfylla sina skyldigheter, om myndigheten inte uppfyller de krav som följer av denna lag eller föreskrifter som meddelats med stöd av den. Av föreläggandet ska framgå vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa de påtalade bristerna.	(INGEN ÄNDRING)	—	—
29 § Om en myndighet allvarligt brister i sin skyldighet att uppfyllade krav som gäller för en behandling av personuppgifter som myndigheten utför, får tillsynsmyndigheten förbjuda myndigheten att fortsätta behandlingen på något annat sätt än att personuppgifter lagras. Ett beslut om förbud mot fortsatt behandling gäller omedelbart.	(INGEN ÄNDRING)	—	—
30 § Tillsynsmyndigheten får hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas.	(INGEN ÄNDRING)	—	—
31 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om 1. när behandling av personuppgifter är tillåten, 2. vilka krav som ställs på en personuppgiftsansvarig myndighet, och 3. att känsliga personuppgifter får behandlas om det behövs med hänsyn till ett viktigt allmänt intresse. Regeringen får meddela föreskrifter om begränsningar av möjligheterna att använda andra sökbegrepp än de som avses i 12 §.	(UTGÅR)	Eftersom behandlingen av uppgifter styrs av verksamheten (6, 8 §§) och verksamheten redan regleras utanför myndighetsdatalagen, finns ingen anledning att ålägga regeringen att utfärda särskilda föreskrifter om personuppgifter. Ändamålsbegränsning, dataminimeringen, transparensen och det effektiva utövandet av rättigheterna i Dataskydd.net:s föreslagna 6 § samt 25a § kan antas vara tillräckliga skyddsmekanismer för individen, som den dessutom själv kan begagna sig av.	s. 13
32 § Tillsynsmyndighetens beslut enligt denna lag om annat än föreskrifter får överklagas till allmän förvaltningsdomstol.Tillsynsmyndigheten får bestämma att dess beslut ska gälla även om det överklagas.	(INGEN ÄNDRING)	—	—

Utredningens förslag	Dataskydd.net:s förslag	Kommentar	Se ovan
33 § Beslut om rättelse eller komplettering enligt 24 §, om avskiljande eller utplåning enligt 25 § och om information enligt 26 § personuppgiftslagen (1998:204) får överklagas till allmän förvaltningsdomstol. Första stycket gäller inte för beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.	33 § Beslut som fattats av myndigheter enligt denna lag eller tillämpliga bestämmelser i personuppgiftslagen får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.	Det är inte tydligt varför de flesta beslut inte ska gå att överklaga. För att privatpersonen ska stärkas i sin egen makt över sig själv, måste den också kunna ifrågasätta maktutövande mot den egna personen.	s. 23-24
34 § Andra beslut enligt denna lag än sådana som avses i 32 § och 33 § första stycket får inte överklagas. Prövningstillstånd krävs vid överklagande till kammarrätten.	(UTGÅR)	Överflödig givet ny formulering i 33 §.	