dataskydd.net

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

Dataskydd.net Sverige
c/o Anders Jensen-Urstad
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Stockholm 2016-11-05

Remissyttrande över SOU 2016:41 – Hur står det till med den personliga integriteten?

Innehåll

Sammanfattning

Den här texten innehåller 13 förslag och ett bestyrkande.

De förslag vi presenterar är kategoriserade efter vilket av delbetänkandets kapitel vi anser bäst påvisar behovet av förslagen. I kommentarerna till kapitel 5 har vi således presenterat två förslag som vi tror kan underlätta Integritetskommitténs arbete med integritetsskydd. Förslagen är färgade av vår förståelse för den europeiska dataskyddslagstiftning som träder i kraft i maj 2018.

I kommentarerna till kapitel 22 (se 5) om informationssäkerhet och kapitel 23 (se 15) om skyddet för den enskilda har vi lagt fram ytterligare förslag, där vi tagit med observationer från både kommitténs delbetänkande och andra statliga utredningar. Vi har försökt anpassa förslagen efter de begränsningar vi ser att Integritetskommittén drabbas av i och med den stora mängden parallellt pågående utredningar. Vi har sammanställt de utredningar vi själva hittat i kapitel 24 (se 23).

Därför finns inga förslag om att stärka möjligheten för enskilda privatpersoner att utöva sina rättigheter till dataskydd och privatliv i forskningsprojekt, statistiska utredningar, i försäkringsväsendet eller marknadsundersökningar trots att delbetänkandet identifierar problem i samband med samtliga dessa områden. Trots att delbetänkandet funnit osäkerhet kring behandling av personuppgifter och integritetsskydd i samband med polisarbete, försvarsunderrättelseverksamhet och säkerhetspolisen har vi inte heller lagt några specifika förslag på dessa områden.

Inga förslag har heller lagts om möjligheten att öka privatpersoners informationssäkerhet genom att sluta sälja identitetsuppgifter eller tillåta att de publiceras på internet för användning av bedragare (se vidare 25). Vi har även undanhållit oss från att lägga förslag om tillsyn, utom i det att vi efterfrågar en markering av att individers rätt till dataskydd och möjlighet för informationssäkerhet bör ges åtminstone lika hög prioritet som statens självupplevda intresse av sådan säkerhet, samt behovet av samtidig juridisk och teknisk kunskap hos till exempel Datainspektionen (se vidare 26.

I vissa fall är våra förslag av en direkt karaktär och innebär att en konkret åtgärd behöver vidtas (till exempel angående individcentrisk incidentrapportering och vidareutbildning av åklagare). I andra fall är förslagen mer principiellt hållna (till exempel att det bör vara tydligare vad effektivisering antas betyda, eller hur man tolkar kriterierna för informationssäkerhet).

Förslagen är listade först i varje avsnitt, och därefter följer längre texter och motiveringar till förslagen. Källförteckningen och fotnötterna bör ses mer som en vägledning till mer information än som en uttömmande katalog av källmaterial för något av de områden vi berör.

Kommentarer och förslag på kapitel 5

Förslag:

1 Kommittén bör förenkla sitt arbete genom att skilja på rätten till dataskydd (artikel 8 i EU:s stadga) och rätten till personlig integritet (artikel 7 i EU:s stadga) på det sätt att man ser dataskydd som en samling verktyg som enskilda individer kan använda för att utöva sin rätt till personlig integritet.

2 Kommittén bör observera att både förordning (EU) 2016/679 (EU:s dataskyddsförordning)[a] och direktiv (EU) 2016/680 (EU:s nya dataskyddsdirektiv)[b] har som följd att svenska medborgares rättigheter vid personuppgiftsbehandling i samtliga verksamheter som de rimligen kommer i kontakt med i sina liv nu faller under EU:s stadga och ovan nämnda uppdelning. Detta ställer i sin tur nya krav på hur regeringen genomför proportionalitets- och nödvändighetsbedömningar även då regeringen utarbetar egna föreskrifter, förordningar och avtal med tredje land.

[a] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning).

[b] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

I DELBETÄNKANDETS kapitel fem framgår att kommittén haft stora problem att definiera begreppet ”integritet”.[1] Av delbetänkandet framgår dessutom att detta har varit ett problem för den svenska lagstiftaren och svenska utredare under en mycket lång tid.[2] Liknande svårigheter finns i arbetet med att definiera rätten till en privat sfär, rätten till privatliv eller rätten till en egen identitet. Alla dessa rättigheter går att härleda till Europakonventionens artikel 8.[3] Både Europakonventionen och EU:s stadga för grundläggande rättigheter har en starkare karaktär av positiva skyldigheter för staten[4] än svenska regeringsformen.[5]

Dataskydd och personlig integritet

EU:S STADGA för grundläggande rättigheter delar till skillnad från andra rättighetsbärande dokument upp den fredade sfären för privatlivet i två separata rättigheter: en rätt till privatliv och privat sfär (artikel 7) och en rätt till data-

[1] Kap. 5.2, SOU 2016:41.

[2] Kap. 5.3, SOU 2016:41.

[3] Europeiska konventionen för mänskliga rättigheter, ETS No.005.

[4] *Se t. ex.* Blog seminar on positive obligations (3): Positive obligations to protect fundamental rights – any role to be played by the European Court of Justice?, Malu Beijer, Radboud University Nijmegen *på* Strasbourg Observers-bloggen 10 oktober 2016.

[5] *Se t.ex.* Elisabet Reimers, Integritetsskyddet i regeringsformen, SvJT 2009 s. 435.
Någon motsvarighet till den rättighetskatalog som Europakonventionen innehåller, vilken i både positiv och negativ bemärkelse förpliktar konventionsstaterna att garantera var och en skydd för fri- och rättigheterna, finns alltså inte i den svenska grundlagen. Skyddet i 2 kap. RF tar i stället sikte på att begränsa riksdagens makt att stifta lag i vissa fall och utgör således enbart en negativ förpliktelse för det allmänna.

skydd (artikel 8). EU-domstolen har framhållit att dessa rättigheter ska tolkas så att artikel 7 i EU:s stadga motsvarar artikel 8.1 i Europeiska konventionen för mänskliga rättigheter.[6] Artikel 8 i EU:s stadga kan i stället tolkas som en samling verktyg genom vilka enskilda privatpersoner ges en möjlighet att utöva rätten till privatliv.

Rätten till privatliv, eller rätten till personlig integritet, eller rätten till en egen självständig identitetsutveckling, är flytande begrepp. Rätten till privatliv eller personlig integritet är subjektiv: det är i någon mening upp till varje människa att bestämma vad deras privata sfär är, och det är svårt för varje annan människa att relatera till vad denna första människa bestämt. Utredningen har observerat detta med hänvisningar till privatlivsforskarna Daniel Solove[7] och Helen Nissenbaum,[8] och det finns otvetydigt en omfattande doktrin kring vad förståelsen för termen "integritet" i olika sammanhang bör vara. Dataskydd.net har ofta använt sig av den historiska kartläggning av olika privatlivsparadigm som sammanställts av Seda Gürses i hennes datavetenskapliga avhandling vid KU Leuven 2010:[9]

1) Integritet som konfidentialitet: att gömma sig,[10]

2) integritet som kontroll – informationellt självbestämmande,[11] och

3) integritet som praktik – identitetsbildning.[12] Nissenbaum faller under Gürses tredje paradigm. Dataskyddslagstiftningen faller, enligt Gürses, mestadels under det andra paradigmet.

Rätten till dataskydd är inte relativ på samma sätt som rätten till privatliv. Rätten till dataskydd bör ses som en samling metoder som privatpersoner kan använda för att upprätthålla och utöva sin rätt till privatliv.[13] Dessa metoder definieras i lagar så som personuppgiftslagen eller EU:s dataskyddsförordning, men också i registerförfattningar, lagar om hemliga tvångsmedel, och så vidare.

Dataskydd är en självständig och separat rättighet enligt EU:s stadga för grundläggande rättigheter. Den kan antas ha sin grund i tyska konstitutionsdomstolen resonemang om "informationellt självbestämmande".[14] Politiskt är det möjligt att konkretisera vilka verktyg man anser att rättigheten ska omfatta. Det vill säga, vilka verktyg man vill ge till privatpersoner att utforska sin privata sfär, identitetsutveckling och åsiktsbildning.

---

[6] WebMindLicenses, C-419/14, EU:C:2015:832, paragraf 70.
[A]rtikel 7 i stadgan, som handlar om rätten till skydd för privatlivet och familjelivet, innehåller rättigheter motsvarande dem som garanteras i artikel 8.1 i Europakonventionen, och att rättigheterna i artikel 7 i stadgan följaktligen, i enlighet med artikel 52.3 i stadgan, ska tillskrivas samma innebörd och samma räckvidd som rättigheterna i artikel 8.1 i Europakonventionen, såsom denna har tolkats av Europeiska domstolen för de mänskliga rättigheterna (dom McB., C-400/10 PPU, EU:C:2010:582, punkt 53, och dom Dereci m.fl., C-256/11, EU:C:2011:734, punkt 70).

[7] SOU 2016:41, s. 137.

[8] SOU 2016:41, s. 138.

[9] Kapitel 2 i Fahriye Seda Gürses, Multilateral Privacy Requirements Analysis in Online Social Network Services, KU Leuven, 2010.

[10] Ibid., kapitel 2.2.2.

[11] Ibid., kapitel 2.2.3.

[12] Ibid., kapitel 2.2.4.

[13] Jämför Europarådets konvention 108 om skydd för individer med hänseende till automatisk behandling av deras personuppgifter, artikel 1.

[14] Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1.

Dataskydd är alltså ett enklare begrepp för lagstiftare att arbeta med och förhålla sig till än vad rätten till privatliv är, eftersom dataskydd inte behöver bedömas i varje enskilt fall eller utefter varje enskild individs kontext. Verktygslådan – och det ansvar som tillfaller samhället att effektivt förvalta verktygslådan – möjliggör också att man löser privatlivsproblem som uppstår vid sådana tillfällen då man behöver väga det globala intresset av ett skyddat privatliv mot enskildas intressen av att vara transparenta med sig själva på ett som sätt påverkar andra enskilda.[15] Det kan vara värt att nämna att aktörer som Helen Nissenbaum,[16] men också säkerhetsgurun Bruce Schneier,[17] argumenterat för europeisk-inspirerade dataskyddslagar även i den amerikanska kontexten.

Nackdelen för Integritetskommittén med just verktygslådan som finns i den europeiska lagstiftningen är att den redan är beslutad i och med de förhandlingar som riksdagen genom sitt ansvarsutkrävande av regeringen bidragit till sedan 2012. Integritetskommittén kan inte utöva något särskilt inflytande över hur rätten till dataskydd bör manifesteras i lagstiftning. På sidan 23 i kommentarerna till delbetänkandets kapitel 24 kommer vi att komma tillbaka till andra sätt vi ser att Integritetskommittén i praktiken är begränsad i vad den kan föreslå.

Kommentarer och förslag på kapitel 22

Förslag:

1 Utredningen bör uttrycka att konsumenters och medborgares intresse av nätverks- och informationssäkerhet ska tillgodoses i minst lika hög utsträckning som det statliga.

2 Utredningen bör föreslå att den svenska lagstiftaren inför det individcentriska incidentrapporteringssystemet som redan är vanligt i amerikanska delstater, och där incidentrapporter ska skickas ut till de privatpersoner som kan ha drabbats av incidenten (misstanke att en individ har drabbats ska alltså vara tillräckligt för rapporteringskrav). Om Datainspektionen inte upplever att sådan rapportering är möjlig under artikel 34 i dataskyddsförordningen, bör kommittén föreslå individcentrisk incidentrapportering som konsumentskyddande åtgärd i enlighet med artikel 169(4) FEUF.

3 Utredningen bör plocka upp Post- och telestyrelsens förslag från 2006 att utveckla näringsorienterad sårbarhetsrapportering. Målsättningen med sådan rapportering är att kunna säkerställa sig om att sårbarheterna snabbt kan åtgärdas. För att ge incitament att inte skjuta på

[15] Se Joshua A. T. Fairfield och Christoph Engel, Privacy as a Public Good. Duke Law Journal, december 2015, Vol. 65 Issue 3, p385-457:

Today's social, legal, and self-regulatory tools [for protecting privacy] focus on empowering individuals. They must equally be focused on empowering groups.

Individual empowerment is not enough because an individual's disclosure of information about herself impacts many other people. One source of risk is immediate and palpable—information about one person is also information about others.

[16] Helen Nissenbaum, Must Privacy Give Way to Use Regulation?, föreläsning på Brown University, 15 mars 2016.

[17] Bruce Schneier, Data is a Toxic Asset, 4 mars 2016.

åtgärdande av sårbarheterna bör dessa offentliggöras efter en viss tidsperiod, som kan anpassas i förhållande till sårbarhetens svårighet men inte vara längre än till exempel ett par år.

4 Utredningen bör observera att begreppet ”*spårbarhet*” innebär att den som blir spårad är den som presumeras göra fel. Hur man implementerar *spårbarhet* och *konfidentialitet* påverkar i allra högsta grad maktbalansen mellan enskilda privatpersoner, företag och myndigheter och är därför ingen trivial teknisk fråga, utan en stor (och inte nödvändigtvis enkel) politisk fråga.

5 Utredningen bör observera att så kallad *beställarkompetens* i första hand skulle kunna tillgodoses genom att skapa en tydligare styrning för dataskydd och informationssäkerhet, särskilt genom att se till att tillsynsmyndigheter som Datainspektionen och Post- och telestyrelsen får tydligare budgetutrymme och mandat för att utfärda riktlinjer och kräva revisioner.

DATASKYDD.NET välkomnar att utredningen observerat just eftersättandet av enskildas informationssäkerhet när åtgärdsprogram och strategier utarbetats. En ytterligare observation kan vara att tekniska åtgärder som behöver vidtas för att skapa informationssäkerhet för organisationer inte nödvändigtvis är sammanfallande med de åtgärder som skapar informationssäkerhet för individer. Målet med säkerheten är avgörande för hur säkerheten implementeras och mäts.[18]

Konsument- och individorienterad informationssäkerhet

FÖR ATT GE konsumenter och enskilda medborgare en högre nivå av informationssäkerhet måste konsumenter och medborgare veta var de kan vända sig med informationssäkerhetsproblem. I dag vänder sig många enskilda till polisen med problem som uppstått till följd av antingen företags eller myndigheters slapphänta dataskydd (till exempel vid identitetskapningar), trots att polisen inte kan åtgärda säkerhetsproblem som uppstår för att privat sektor inte investerar tillräckligt mycket i informationssäkerhet, eller att myndigheter eftersätter

[18] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (2d ed. 2008). Till exempel detta abstrakt ur kapitel 1:

The conventional view is that while software engineering is about ensuring that certain things happen (‘John can read this file’), security is about ensuring that they don’t (‘The Chinese government can’t read this file’). Reality is much more complex. Security requirements differ greatly from one system to another. One typically needs some combination of user authentication, transaction integrity and accountability, fault-tolerance, message secrecy, and covertness. But many systems fail because their designers protect the wrong things, or protect the right things but in the wrong way. /.../

There is a lot of terminological confusion in security engineering, much of which is due to the element of conflict. ‘Security’ is a terribly overloaded word, which often means quite incompatible things to different people.

To a corporation, it might mean the ability to monitor all employees’ email and web browsing; to the employees, it might mean being able to use email and the web without being monitored. As time goes on, and security mechanisms are used more and more by the people who control a system’s design to gain some commercial advantage over the other people who use it, we can expect conflicts, confusion and the deceptive use of language to increase.

privatpersoners informationssäkerhet.[19]

Det skulle kunna hjälpa om lagstiftaren undanhöll sig från att flytta ansvaret för informationssäkerhet från huvudsakligen konsument- och marknadsorienterade myndigheter (så som Post- och telestyrelsen och Datainspektionen) till en i huvudsak statsorienterad myndighet (så som Myndigheten för samhällsskydd och beredskap) så som man gjorde med CERT-SE (se vidare sidan 11). Huvudmannens uppdrag påverkar tolkningen av säkerhetsbegreppet och därför dess nytta för enskilda privatpersoner och konsumenter, samt deras kommersiella transaktionspartners.

Individcentrisk indicidentrapportering

Individcentrisk incidentrapportering finns i dag i 47 amerikanska delstater[20] och innebär att enskilda privatpersoner har en rätt att underrättas om IT-säkerhetsproblem som riskerar att ha drabbat dem. Ibland är rättigheten avgränsad till vissa sektorer (till exempel hälso- och sjukvård eller finansindustrin) och ibland är förpliktelserna mer omfattande (till exempel utsträckta även till sociala nätverk, e-postadresser och telefonnummer).[21] En variant på individcentrisk rapportering finns även i EU:s dataskyddsförordning.[22]

Individcentrisk incidentrapportering har givit upphov till tjänster riktade till privatpersoner där de kan utvärdera leverantörer av IT-tjänster efter hur väl de hanterar informationssäkerhetsproblem.[23]

Även om kvantitativa studier indikerar att bara ett fåtal individer ställer leverantörer till svars i domstol,[24] finns det marknadsundersökningar som indikerar att konsumenternas förtroende stärks för de leverantörer som berättar för konsumenter när de haft dataläckor och att de även har en strategi för att hantera dessa.[25] Detta har redan uppmärksammats i ett bidrag till Digitaliseringskommissionens temarapport från juli 2016.[26]

De europeiska incidentrapporteringsbestämmelserna har ett annat fokus än de amerikanska. I Sverige har man framför allt fokuserat på Myndigheten för samhällsskydd och beredskaps möjligheter att tillverka statistik över inträf-

[19] *Se t. ex.* Amelia Andersdotter, ”Innan vi petar i brottsbalken borde vi ta en förnyad titt på konsumenträtten”, Dagens juridik, 22 mars 2016 *samt* Amelia Andersdotter, ”Hot mot personlig säkerhet och integritet - i Sverige räcker det med att vara folkbokförd”, Dagens juridik, 19 september 2016 *samt* Amelia Andersdotter, ”E-legitimationslösning för tvångsregistrerade - ett större förvaltningsrättsligt problem”, Dagens juridik, 24 oktober 2016.

[20] National Conference of State legislatures. Security Breach Notification Laws. [http://perma.cc/7EDG-KVBF].

[21] Steptoe & Johnson LLP, Comparison of US State and Federal Security Breach Notification Laws – Current through January 21, 2016. http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

[22] Artikel 33-34, förordning (EU) 2016/679.

[23] *Jfr* ”Privacy Rights Clearinghouse”, en amerikansk konsument-inriktad hemsida om dataläckor och IT-incidenter. https://www.privacyrights.org/data-breach, *men se också* ”Have I been pwned?”, som dock inte ger meningsfulla sätt att aggregera data eller ställa ansvariga aktörer till ansvar. https://haveibeenpwned.com/.

[24] En översyn av stämningar finns i Sasha Romanosky, David Hoffman, Alessandro Acquisti, ”Empirical Analysis of Data Breach Litigation”, WEIS 2012 samt i författarnas senare artikel ”Empirical Analysis of Data Breach Litigation”, Journal of Empirical Legal Studies, 2014, volym 11(1), 74–104. Se även Rachel M Peters, ”So you’ve been notified, now what? – The problem with current data breach notification laws”, Arizona Law Review. 2014, Vol. 56 Issue 4, p1171-1202.

[25] Deloitte, Deloitte Australian Privacy Index 2015: Transparency is opportunity.

[26] Erik Lakomaa, ”Digitaliseringen, förtroendet, företagen och konsumenterna” i Digitaliseringskommissionen, Temarapport 2016:1, Det datadrivna samhället.

fade incidenter.[27] Lagstiftningen om incidentrapporter för tillhandahållare av elektroniska kommunikationsnät i EU:s förordning ger Post- och telestyrelsen möjlighet att inleda tillsyn,[28] men innebär inga avsevärt förbättrade möjligheter för enskilda att hålla leverantörer ansvariga för säkerhetsfel.[29] Det europeiska nätverks- och informationssäkerhetsdirektivet[30] har återigen ett fokus på en tillsynsmyndighets möjligheter att bilda sig en statistisk uppfattning om vilken sorts incidenter som äger rum, snarare än möjligheter för individer att utkräva ansvar för inträffade incidenter. Inte heller den väntade ändringen att dataläckor som rapporteras till Myndigheten för samhällsskydd och beredskap även ska delas med polisen kan antas förbättra enskilda individers möjlighet att utkräva ansvar vid dataläckor.[31] Dataskydd.net har överklagat CERT-SE:s sekretessklassning av samtlig information i incidentrapporter som enheten vid Kammarrätten i Göteborg, men målet är ännu inte avgjort.

Även om det i den nya dataskyddsförordningen[32] finns bestämmelser i artikel 34 om incidentrapportering till enskilda, finns begränsningar på de omständigheter under vilka individer ska informeras. Ett inträffat säkerhetsproblem ska ”*sannolikt leda till hög risk för fysiska personers rättigheter*” innan en enskild behöver informeras om det inträffade problemet.

Begreppen ”sannolikt” och ”hög risk” kommer att tolkas av Datainspektionen och andra europeiska tillsynsmyndigheter. Det finns i princip inget som förhindrar att de tolkar bestämmelsen på ett sådant sätt att EU:s allmänna dataskyddsförordning utsträcker liknande rättigheter till europeiska konsumenter som amerikanska konsumenter redan har. En förstudie beställd av Konsumentverket om konsumentfrågor och digitalisering markerar att just bristande insyn är ett stort problem för konsumenter.[33] Tillsynsmyndigheternas självständighet begränsar dock det politiska handlingsutrymmet att formellt styra deras tolkning av enskildas rättigheter enligt artikel 34.

För att den svenska lagstiftaren ska kunna föreslå starkare rättigheter för enskilda i incidentrapportering, till exempel för att man vill bättre följa den amerikanska utvecklingen med starkare tonvikt på enskilda individers egna möjlighet att utkräva ansvar vid inträffade säkerhetsfel, så skulle den svenska lagstiftaren behöva skapa inhemsk lagstiftning som går längre än den europeiska.

Artikel 169(4) FEUF om att varje medlemsland har en rätt att skapa starkare inhemska regler till skydd för konsumenter än vad som ingår i det europeiska regelverket är en öppning för att gå längre än vad dataskyddsmyndigheterna kan tänkas göra.

ARTICLE 29
Data Protection Working Party

Tillsynsmöjligheter. Det är Datainspektionen och deras europeiska kollegor i Artikel 29-gruppen som kommer att bestämma i vilken utsträckning dataskyddsförordningens regler om incidentrapportering kommer att innebära ett större eller ett mindre steg framåt för ansvarsutkrävande.

Fördraget om EU:s funktionssätt (FEUF). Avdelning XV Konsumentskydd.

Artikel 169 (f.d. artikel 153 FEG).

1. För att främja konsumenternas intressen och säkerställa en hög konsumentskyddsnivå ska unionen bidra till att skydda konsumenternas hälsa, säkerhet och ekonomiska intressen samt till att främja deras rätt till information och utbildning och deras rätt att organisera sig för att tillvarata sina intressen.
2. Unionen ska bidra till att uppnå de mål som avses i punkt 1 genom
a) åtgärder som beslutas enligt artikel 114 inom ramen för förverkligandet av den inre marknaden,
b) åtgärder som understöder, kompletterar och övervakar medlemsstaternas politik.
3. Europaparlamentet och rådet ska i enlighet med det ordinarie lagstiftningsförfarandet och efter att ha hört Ekonomiska och sociala kommittén besluta om de åtgärder som avses i punkt 2 b.
4. Åtgärder som beslutas enligt punkt 3 ska inte hindra någon medlemsstat från att upprätthålla eller införa strängare skyddsåtgärder. Sådana åtgärder måste vara förenliga med fördragen. Kommissionen ska underrättas om åtgärderna.

[27] Myndigheten för samhällsskydd och beredskap, Obligatorisk it-incidentrapportering.

[28] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) *samt* Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation.

[29] SOU 2016:41, s. 620–621.

[30] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

[31] Ds 2016:22 Polisens tillgång till information om vissa it-incidenter.

[32] Se ovan fotnot *a*.

[33] *Se* Konsumentverket, Rapport 2016:12 Digitalisering och konsumentintresset, s. 10, samt genomgående.

Näringslivsinriktad sårbarhetsrapportering

Post- och telestyrelsen lyfte frågan om sårbarhetsrapportering redan i sin strategi för ett säkrare internet i Sverige från 2006,[34] alltså innan de i och för sig genom EU-rätten garanterades en rätt att veta när IT-säkerhetsproblem hade inträffat genom EU:s uppdaterade förordning om uppgiftsskydd i elektroniska kommunikationsnät.[35] Integritetskommittén har själv identifierat svårigheterna för Post- och telestyrelsen i att agera på incidentrapporterna de tar emot.[36] Om ett befintligt och granskat problem åtgärdas på ett hafsigt och slarvigt sätt som riskerar att i framtiden vara till men för konsumenter, kan Post- och telestyrelsen inte göra annat än att vänta på att den hafsiga och slarviga lösningen leder till ett nytt problem. Ett möjligt svar som utvecklats i EU är förpliktelsen på vissa näringslivsaktörer i bassektorer och eventuellt molntjänster att implementera säkerhetsåtgärder och -processer som föreslagits av en utsedd tillsynsmyndigheter.[37] Detta är emellertid otillfredsställande.

Produktcyklerna i IT-industrin är väldigt korta, ofta kortare än en certifieringsprocess. En myndighet som på förhand dikterar åtgärder riskerar att ha ett kunskapsundertag i förhållande till företagen som arbetar med sina lösningar varje dag. Ett sätt att ta sig runt problemet är transparens: genom att företag incentiveras eller tvingas rapportera problem, får företagen ett tryck på sig att utveckla lösningar för sina problem. Rapporter bör göras allmänt tillgängliga, gärna inom någon tidsgräns (som dock kan vara lång, säg ett par år).

Även i näringslivet har det utvecklats många metoder för säkerhet som förlitar sig på transparens kring just säkerhetsproblem. I stället för att ty sig till straffrätten eller administrativa förhandsgranskningar av åtgärder (vilka är de lösningsmodeller man framför allt tillämpar i svensk förvaltning i dag), läggs en större tonvikt på öppenhet med och små gradvisa förbättringar av hantering av IT-säkerhetens utmaningar.

Bug bounty awards, ett sätt att dela ut belöningar till dem som hittar sårbarheter i IT-system, har till exempel blivit vanliga.[38] Utbyte av information om sårbarheter inom företagsnätverk som ISAC:s har blivit ett vanligare sätt att snabbt ta hand om säkerhetsproblem som annars skulle drabba många i samma industri.[39]

Andra exempel är Google Project Zero, som utreder och publicerar sårbarheter i både Google-system och andra system. Det finns standardiserade databaser där kända sårbarheter publiceras för hela världen att granska och se, till exem-

[34] Post- och telestyrelsen. Strategi för ett säkrare Internet i Sverige, PTS-ER-2006:12:

> *Ett av de största problemen på Internet idag är den bristande säkerheten i de enskilda Internetanvändarnas miljöer. Datorer som inte är tillräckligt skyddade kan utan användarens kännedom övertas, fjärrstyras och därmed utnyttjas som plattformar för överbelastnings- och störningsattacker mot bland annat kritiska delar av Internets infrastruktur. Detta innebär inte enbart en risk för den enskilde användarens integritet eller egendom, utan även för Internets funktion i stort. /.../*
>
> *Det är viktigt att användare av program och protokoll bevakar sårbarheter för de program och protokoll som de nyttjar. Genom att tidigt uppmärksamma sårbarheter som berör egna system kan de snabbare undvikas.*

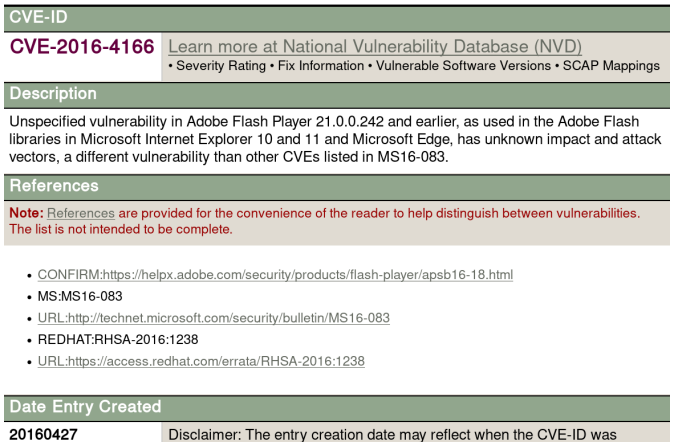
[35] Se ovan fotnot 28.

[36] Kap. 23.2.2, SOU 2016:41.

[37] Artikel 14.1 och 16.1 i direktiv (EU) 2016/1148 (se ovan fotnot 30).

[38] Se till exempel https://bugcrowd.com/list-of-bug-bounty-programs

[39] CIRCL.lu, Malware Information Sharing Platform MISP - A Threat Sharing Platform. https://www.circl.lu/services/misp-malware-information-sharing-platform/; National Council of Information Sharing and Analysis Centers, http://www.nationalisacs.org/



CVE-ID

CVE-2016-4166 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://helpx.adobe.com/security/products/flash-player/apsb16-18.html
- MS:MS16-083
- URL:http://technet.microsoft.com/security/bulletin/MS16-083
- REDHAT:RHSA-2016:1238
- URL:https://access.redhat.com/errata/RHSA-2016:1238

Date Entry Created

20160427 Disclaimer: The entry creation date may reflect when the CVE-ID was

CVE – Common Vulnerabilities and Exposures system. Så här kan en buggrapport se ut i MITRE:s CVE-system, ett öppet system för säkerhetsfel med standardiserade felrapporter som gör det enklare för utvecklare världen över att hitta och åtgärder säkerhetsfel i mjukvaror. Innan CVE-systemet fanns var det vanligt att olika länder eller företag hade olika sätt att beskriva och namnge samma säkerhetsfel. Det gjorde att det blev svårt att dela erfarenheter och åtgärda problem snabbt. Man kan själv undersöka databasen på `https://cve.mitre.org`.

pel MITRE-institutets Common Vulnerabilities and Exposures-system (CVE). Öppen publicering (under vissa villkor) ses ofta som en förutsättning för att säkerhetsproblemen som följer av sårbarheterna ska åtgärdas.

Till skillnad från många äldre akademiska discipliner präglas dataveten-skapen och säkerhetsekonomisk forskning av öppna publiceringar: det är till exempel vanligare att forskare presenterar sina resultat på konferenser än att de låter publicera sig i slutna tidskrifter. WEIS, IEEE Security and Privacy, Chaos Communication Congress och Black Hat är exempel på sådana konferenser.

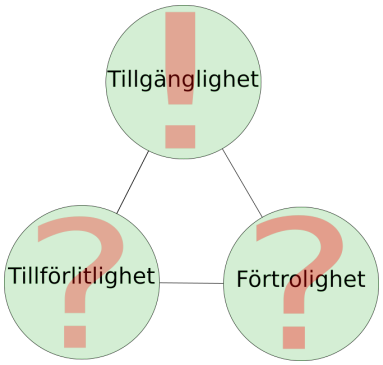
Sårbarhetsrapportering är inget trivialt område att närma sig. De företag som redan tillämpar transparensbaserade modeller för inkrementella IT-säkerhetsförbättringar kommer sannolikt inte att välkomna obligatoriska rapporteringskrav, och de företag som helst slipper åtgärda säkerhetsproblem har inte heller något intresse av att rapportera sina sårbarheter. Utvecklingen av lagstiftning om nya tvångsmedel ser snarare ut att leda till att brottsbekämpande instanser i samhället kommer att få starka operativa incitament att förhindra företag från att avslöja och åtgärda säkerhetsproblem allt för snabbt.[40]

Om Integritetskommittén är intresserad av att lyfta detta förslag (vilket Dataskydd.net rekommenderar) skulle kommittén göra bra i att ta till vara på erfarenheterna från Luxemburgs industriorienterade (och därför näringspo-

[40] Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI): Skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan, Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI): Skrivelse till den pågående utredningen om hemlig dataavläsning. Ur inledningen:

> *Utredningen har att ta ställning till behovet av hemlig dataavläsning. Vi kommer i anslutning till detta uppdrag att beskriva konsumenters svaga ställning i elektroniska miljöer och rätten till identitet som en förlängning av rätten till privatliv och dataskydd. Utifrån vår behandling kommer vi att dra slutsatsen att utredarens uppdrag riskerar att allvarligt skada konsumenters och enskildas intressen och rättigheter i digitala miljöer, och att införandet av ett nytt tvångsmedel knappast är e fektivt i sam- hällelig bemärkelse om inte konsumenter allra minst ges juridisk säkerhet i en utsträckning som kompenserar för den bortfallna tekniska säkerhet som kan väntas resultera av att brottsbekämpande myndigheter får ett operativt incita- ment att utnyttja, hemlighålla och bevara sårbarheter.*

litiskt styrda) CERT.[41] I praktiken skulle detta kunna manifesteras genom att man återupprättar SITIC under Post- och telestyrelsen och initierar ett *responsible disclosure*-program. Notera att CERT-SE på grund av sin placering under Myndigheten för samhällsskydd och beredskap får sina uppdrag från Justitiedepartementet, och att de därför blir mer rättspolitiskt styrda än näringspolitiskt. Det påverkar CERT-SE:s möjligheter att interagera med privat sektor negativt.



Säkerhetstriad. I Utredningen om den Europeiska IT-brottskonventionen (SOU 2013:39) använder man sig av begreppen förtrolighet, tillförlitlighet och tillgänglighet för att beskriva den sortens informationssäkerhet man vill uppnå med hjälp av IT-brottslagstiftning. Tillförlitlighet borde motsvara riktighet. Förtrolighet borde motsvara konfidentialitet. Tillgänglighet betyder att medborgarna kan ta del av sådan information som myndigheten eller företaget har avsett att de ska kunna ta del av.

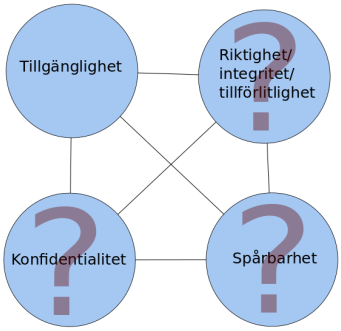
Spårbarhet och konfidentialitet

Den nederländska juridikforskaren Axel Arnbaks avhandling om säkerhet och ekonomi i europeisk lagstiftning går igenom hur lagstiftaren ofta fokuserat på IT-systemens tillgänglighet (till exempel åtgärder som garanterar en viss upp-tid på en server, så som att en webbplats eller databas är tillgänglig och går att nå över ett kommunikationsnät) men eftersatt riktighet och konfidentialitet när lagstiftaren utarbetat lagstiftning om säkerhet i elektroniska miljöer. Arnbak menar att detta lett till att den sortens säkerhet som är viktigast för konsumenter inte har fått något stort utrymme i säkerhetslagstiftningen.[42]

Arnbaks rekommendationer är att vara tydlig med vad säkerhetsbegreppet innebär (vem eller vad ska skyddas, och från vem eller vad ska detta första vem eller vad skyddas). Arnbak lyfter också transparens för marknadens aktörer som en viktig utgångspunkt för konsumenter och stater för att effektivt kunna lagstifta om, och upprätthålla lagstiftning om, datasäkerhet.

I Integritetskommitténs skildring av grundläggande begrepp ur informationssäkerheten har man, i stället för att använda den klassiskt och internationellt etablerade så kallade ”CIA-triaden” (som Arnbak utgår ifrån), använt sig av begreppen *tillgänglighet*, *riktighet* (jämför ”*integrity*”), *konfidentialitet* och *spårbarhet*. Denna kvadrupel är hämtad från NISU-utredningen[43] och avviker från den triad man normalt använder sig av när man förbereder till exempel svensk straffrätt.[44] Anledningen till detta borde vara att IT-brottsstraffrätten har uppnått en hög nivå av internationell harmonisering, medan informationssäkerhet i övrigt fortfarande ses som en nationell polisiär, militär eller krisförberedande angelägenhet. Oavsett om man använder tre eller fyra grundbegrepp i sitt informationssäkerhetsarbete behöver man dock observera att begreppen får olika innebörd beroende på *vem* man skyddar från *vad*.

Det gör skillnad om man företrädesvis skyddar statens och förvaltningens intressen, eller individers intressen. Konfidentialitet eller förtrolighet är till exempel kontextberoende: det gör skillnad vad man håller hemligt från vem



Säkerhetskvadrupel. Om man i internationell rätt har en *säkerhetstriad*, arbetar man nationellt i Sverige snarare utefter en *säkerhetskvadrupel*. Detta medför inte något större fokus på enskilda individers roll, rättigheter och intressen av hur de fyra kriterierna för säkerhet uppfylls. Det fjärde kriteriet *spårbarhet* används tvärtom ofta som ursäkt för att kartlägga enskilda privatpersoner ännu mer, så att de inte stör det allmännas uppfyllande av sina egna behov enligt de tre första kriterierna.

[41] Se ovan fotnot 39.

[42] Axel M. Arnbak. ”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives” doktorsavhandling, Universiteit van Amsterdam, 2015. Från s. 346:

> *Current political dynamics seem to point at quite different ambitions of the EU lawmaker than protecting the communications security interests of end users. Security requirements are watered down, and availability and continuity of the economy are prioritized, rather than the confidentiality and integrity interests that need to be safeguarded through legislation, as the study argued. The scope of EU law still does not cover essential stakeholders in communications value chains, and oversight mechanisms are sought to be placed within the national security establishment of Member States.*

[43] SOU 2015:23 Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.

[44] Se till exempel SOU 2013:39, Europarådets konvention om it-relaterad brottslighet.

och varför.[45] I Sverige väljer vi ofta att tolka ”förvaltningen” som ett enda stort väsen: sekretessbegränsningarna mellan myndigheter är förhållandevis få, och skulle man behöva bryta sekretessen är alla myndighetsregister upprättade på ett sådant sätt att detta tekniskt kan åstadkommas utan problem. I Tyskland har man i stället valt att dela upp förvaltningen på ett sådant sätt att det i princip inte är möjligt att bryta sekretessen mellan myndigheter ens med stora tekniska ansträngningar.

Ur en medborgares perspektiv kan det vara obehagligt att flera större myndigheter har en uppgiftsförsäljning som gör det lätt att kapa identiteter (till exempel i förhållande till fakturabedrägerier, se pizzaexemplet från Örebro på sidan 17). Det kan ses som ett brott mot konfidentialitetsprincipen ur ett medborgerligt perspektiv. Ur Skatteverkets perspektiv blir det dock tillräckligt att deras API[46] är konstruerat på ett sådant sätt att mottagaren av uppgifterna är den som Skatteverket förväntar sig att den ska vara. Stora delar av näthatsutredningen (SOU 2016:7) handlar om information som i och för sig inte behöver vara osann, men som ändå kan vara integritetskränkande om den sprids. Information som myndigheter sparar och delar ut om privatpersoner borde kunna tillhöra denna kategori (se även om Mediagrundlagsutredningen på sid.).

Vad en ”riktig” uppgift är går också att diskutera. Integritetskommittén har kartlagt myndigheternas profilering[47] och användning av automatisk datainsamling från webbplatser.[48] Om man med algoritmer fattar ett beslut (det vill säga, tar fram en uppgift om en viss persons karaktär) baserat på saker man hittat på internet – även om uppgifterna i och för sig hämtades på öppna webbplatser eller sociala plattformar – är det inte längre fråga om en riktighet som går att bevisa till 100%, utan om en hypotetisk riktighet. Där spelar det stor roll vem som presumeras ha rätt: den som hade en dator som genomförde den statistiska beräkningen, eller den som lider negativa konsekvenser av att den statistiska beräkningen genomfördes på ett visst sätt.

Spårbarhet är ett typiskt svenskt kriterium i informationssäkerhet. Spårbarhet ska garantera ansvarsutkrävande. Det gör alltså stor skillnad vem man upplever ska kunna utkräva ansvar av vem. Om det är det allmänna som ska kunna utkräva ansvar av allmänheten för att allmänheten misstänks ägna sig åt bedrägliga beteenden så som överdrivet frekventa inloggningar på e-tjänster, överdrivet många förfrågningar om allmän handling eller felaktig användning av bidrag, kommer man få en annan sorts spårbarhet än om man till exempel vill att allmänheten ska kunna veta att det allmänna inte bryter mot konfidentialitetsbestämmelser, sekretess, eller genomför en orättvis eller diskriminerande behandling av en enskild. Spårbarhet uppnås via loggning.

Tobias Pulls från Karlstads universitet visade 2015 i sin avhandling i datavetenskap hur man genomför loggning på ett sådant sätt att enskildas rätt till dataskydd och integritet kan upprätthållas, samtidigt som man får spårbarhet

[45] Se även ovan, fotnot 18.

[46] *Application Programming Interface*. En specifikation för hur olika applikationsprogram kan använda och kommunicera med en specifik programvara. API:et är ett gränssnitt mellan applikationen och programvaran. Programvaran blir en mjukvarukomponent i applikationen och utgörs vanligen av en uppsättning funktioner, datatyper eller variabler som är tillgängliga för applikationen att använda. Programvarans funktioner kan i sin tur använda funktioner, datatyper och variabler som inte har gjorts tillgängliga för applikationen, utan som är inkapslade i API:et.

[47] SOU 2016:41, kapitel 11.1.9.

[48] SOU 2016:41, kapitel 11.1.10 och 18.7

visavi de organisationer som kan påverka eller missbruka information om enskilda. Särskilt innebär hans forskning att man kan genomföra sådan loggning på ett säkert sätt. Pulls avhandling bevisar möjligheten – och implementerar en metod – för transparent loggning samtidigt som enskilda privatpersoners dataskydd upprätthålls och inte gör det svårare för enskilda individer att utöva sin rätt till privatliv.[49]

Utgångspunkten för hans forskning är att det är en bra idé att genomföra så kallad *transparency logging*. Denna sorts loggning innebär att myndigheter och företag strävar efter att ge spårbarhet för privatpersoner kring hur deras personuppgifter behandlas av organisationen. För att uppnå det målet måste man först och främst minimera tillit till organisationen. Om denna vill göra något fel, eller om den får ett oväntat problem, kan organisationen nämligen sannolikt komma att försöka sopa igen alla spår efter sitt misstag, till exempel för att slippa administrativa sanktionsavgifter enligt EU:s dataskyddsförordning.

Enligt Pulls är en betydelsefull del av integritetsskyddande loggning (att man skapar ett "spår" över de interaktioner som har skett) att uppgifterna i loggen är *olänkbara* till de privatpersoner som givit upphov till spåren.[50] I avhandlingens sjunde kapitel[51] återknyter Pulls sina transparenta och privatlivsskyddande loggar till sådana projekt för e-handel och molntjänster som Dataskydd.net redan tidigare framhållit: Primelife[52] och A4Cloud.[53]

Spårbarhet implementeras mot den aktör man är rädd för och vill kunna utkräva ansvar av om den felar. Genom att lägga fokus på att enskilda individer ska spåras – vilket gjorts i till exempel de lösningar för e-legitimation som utretts av E-legitimationsnämnden och som Integritetskommittén konstaterat används i svensk förvaltning och svenskt bankväsende[54] – har man också implicit godtagit utgångspunkten att det är enskilda individer som kan, vill och är beredda att skada system som dessa ingår i, medan motsvarande möjlighet för missbruk inte finns åt andra hållet. Dataskyddslagstiftningen har av naturliga skäl ett annat fokus, och både uppstod och finns kvar för att skydda individer mot sådant skadligt inflytande som ett system kan utöva över dem.

Detta gäller även konfidentialitet. Dataskyddslagstiftningens utgångspunkt är att individer ska ha en rätt att veta hur deras data sprids, ha en möjlighet att motsätta sig detta och kunna förstå konsekvenserna av hur deras uppgifter sprids. Om individer inte förstår detta är konfidentialitetsprincipen inte uppfylld ur individens synpunkt. Svenska myndigheter är i princip konstruerade på motsatt sätt: individernas förväntas vara intresserade av någon sorts resultat, men ges ingen möjlighet att förstå vilka element som ingår i processen fram till det resultatet.[55] Resultatlösa processer – till exempel att en enskild privatpersons uppgifter delas utan att det egentligen var nödvändigt eller hade något syfte – är svåra att få reda på eller granska. Den informationssäkerhet som förespråkas inom de nuvarande svenska politiska processerna är tänkta att skydda staten mot otillbörlig insyn från aktörer utanför staten (till exempel andra stater), inte att skydda individerna från otillbörlig genomskinlighet mot staten.

[49] Tobias Pulls. "Preserving Privacy in Transparency Logging", doktorsavhandling, Karlstads universitet, 2015.
[50] Ibid, s. 19.
[51] Ibid, s. 143 ff.
[52] https://www.primelife.eu
[53] https://www.a4cloud.eu
[54] SOU 2016:41, kapitel 11.1.11.
[55] Se även E-delegationens slutbetänkande.

Konceptet med olänkbarhet är i princip främmande för svensk statsförvaltning. Som Integritetskommitténs tekniska utredning i bilaga 3[56] visar är olänkbarhet inte heller någonting som svenska säkerhetsingenjörer i någon större utsträckning har tillägnat sig. Det följer ett, enligt Dataskydd.net, ”typiskt svenskt” mönster där enskilda individers intresse av informationssäkerhet sitter i baksätet för lagstiftarens och förvaltningens intressen, medan förvaltningens egna intresse av informationssäkerhet sitter i förarsätet.[57]

Eftersom Dataskydd.net har individers rättigheter i digitala miljöer som fokusområde är vi så klart inte glada över det nuvarande läget.

Beställarkompetens

Beställarkompetens förs ofta upp i IT-upphandlingsdiskussioner för att man upplever sig inte ha sådan kompetens. Det skiljer sig från *in house*-kompetens, i det att beställarkompetensen handlar om att kunna utvärdera erbjudanden från privat sektor snarare än att förstå hur man själv skulle utveckla den sortens IT-system man vill ha. Den typiska statliga lösningen på problemet med bristande beställarkompetens är att man föreslår centralisering av beställningarna, och så har det varit sedan de automatiska datasystemens introduktion på 1970-talet.[58]

Det kan vara sant att det större befolkningsunderlaget i storstäder tillåter enklare rekrytering av personal med högre kompetens. En risk med centralisering är dock att man får felaktiga beslut om IT-infrastruktur som är svåra att ändra och som drabbar väldigt många personer samtidigt.

Ett problem Dataskydd.net har mött när vi har jobbat med kommuner kring dataskyddsfrågor[59] på webbplatser är att kommunerna upplever att de statliga riktlinjerna är otillfredsställande. Tillsynsmyndigheterna i Stockholm tar ofta sikte på formellt överensstämmande med lagstiftningen, varefter rekommendationerna tvingas landa i att den tekniska implementationen av dataskydd ”beror på”. Dataskydd.net har här kunnat ge tydligare svar, då vi verkar för att dataskydd till lika delar ska upprätthållas av juridisk och teknisk implementation.

Lagstiftningen är skriven för att ge stor flexibilitet till dem som har resurser att tolka lagen enligt sina egna preferenser. För aktörer med relativt få resurser och vars huvudintresse kanske är ett annat än att tolka dataskyddslagstiftning på ett för egen del gynnsamt sätt blir flexibiliteten i stället en börda, eller ett hinder för att själv dra snabba slutsatser om vad som är bästa möjliga implementation.

En lösning är att ge myndigheter som Post- och telestyrelsen eller Datainspektionen i uppdrag att utforma riktlinjer och checklistor som gör det tekniskt lätt att förhålla sig till vad som är mer (eller mindre) gynnsamt för dataskydd. Till exempel kan de redan befintliga checklistorna för inbyggt integritetsskydd[60] och säkerhet vid personuppgiftshantering[61] utgöra definitiva kriterier mot vilka kommuner och landsting ska utvärdera produkter som erbjuds dem. En annan

[56] Kirei 2015:20 Integritetsskyddande teknik.

[57] Jfr Riksrevisionens utredningar hänvisade i fotnot 86 eller SOU 2015:23 (NISU-utredningen) i fotnot 43, m.fl.

[58] *Jfr* SOU 1976:69, Teknikupphandling.

[59] *Se* `https://dataskydd.net/kommuner/`

[60] Datainspektionen. Inbyggt integritetsskydd. `http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/`

[61] Datainspektionen. Säkerhet vid personuppgiftshantering. `http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sakerhet-enligt-personuppgiftslagen/`

lösning som Dataskydd.net tittar på är att använda sig av befintliga utvärderingsmekanismer från datavetenskapen, så kallade *privacy metrics* eller *security metrics*, för att rangordna olika tekniska lösningar.[62] Det skulle kräva att myndigheternas kompetenser, särskilt Datainspektionens kompetenser, utökas med till exempel statistisk och datavetenskaplig expertis.

Kommentarer och förslag på kapitel 23

Förslag:

1. Utredningen bör föreslå högre skadestånd för dataskyddsintrång.
2. Utredningen bör underlätta konsumenters och enskilda privatpersoners praktiska möjlighet att visa att personuppgifter har samlats in och behandlats i strid med lagstiftningen.
3. Utredningen bör överväga möjligheten att klaga på myndigheters och företags åtgärder med personuppgifter *in abstracto*, samt överväga hur man kan förbättra möjligheterna för grupptalan. Utredningen kan också överväga att införa en dataskyddsombudsmannafunktion, liknande den som finns på diskrimineringsområdet.
5. Utredningen bör föreslå att åklagare och domare utbildas i dataskyddsrätt.
6. Utredningen bör föreslå att man ser över myndigheternas ekonomistyrning.
7. Utredningen kan förmodligen inte göra annat än uttrycka en förhoppning om att ordet ”effektivisering” ges en tydligare innebörd vid de tillfällen då man anser effektiviseringar vara en anledning att inskränka till exempel dataskydd.

Högre skadestånd vid dataskyddsfel

Den tidigare observationen att skadestånd och andra ekonomiska styrmedel inte kan ha en moralbildande och preventiv funktion[63] motsägs av privata sektorns reaktioner på de höjda administrativa avgifterna som introducerats i EU:s dataskyddsförordning.[64]

Det av integritetsutredningen identifierade exemplet med kvinnan som i och för sig fick rätt mot landstinget i fråga om kränkning av hennes rättigheter enligt personuppgiftslagen, men sedan ändå, efter att ha mottagit sitt skadestånd på sammanlagt 11 000 kronor, fick betala ytterligare 1 365 832 kronor på grund av att tingsrätten ålade henne att stå för landstingets rättegångskostnader.[65] Med sådana pyrrhussegrar är det lättare att föreställa sig att skadeståndens

[62] *Jfr* Isabel Wagner och David Eckhoff, Technical Privacy Metrics: a Systematic Survey, arXiv:1512.00327 [cs.CR].

[63] SOU 2016:41, s. 622–623.

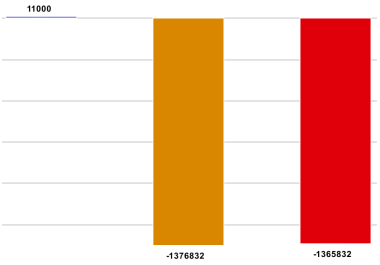
[64] Simon Camponello, EU:s nya datalagar är klara – miljardböter för it-företag som missköter sig, IDG (17 december 2015).

[65] SOU 2016:41, s. 626.

moralbildande och preventiva funktion är att avskräcka enskilda individer från att hävda sin rätt mer än något annat.

För att organisationer som myndigheter och företag ska ha incitament att ta tag i sådana organisatoriska och tekniska åtgärder som krävs för att dataskyddet, integriteten och informationssäkerheten ska ligga på en rimlig nivå behöver det helt enkelt vara dyrare att slarva än att låta bli. För att man ska övertyga sig om detta närmare borde det egentligen räcka med att analysera vad NISU-utredningen ansåg vara resultatet av över 10 års intensivt statligt arbete med informationssäkerhetsstrategier.[66]

Det är ett välkänt problem att det saknas ekonomiska incitament för informationssäkerhetsåtgärder,[67] och att dessa åtgärder om de vidtas kan variera väldigt i kostnad för organisationen som genomför förändringarna[68] samt



Orimliga risker. Enligt delbetänkandet är det följande riskkalkyl man har att förhålla sig till som enskild, när man bestämmer sig för om man ska hävda sin rätt. Vänsterstapeln indikerar skadeståndet man får för att ha blivit kränkt (enligt utredningen ett av de högre skadestånden som kan betalas ut för integritetskränkning). Mittenstapeln är rättegångskostnaderna man får betala åt landstinget, och högerstapeln är den totala summan man som enskild behöver uppbära om man hävdar sin rätt när man blivit kränkt. Exemplet indikerar att skadestånden sannolikt borde vara mer än *hundratalet gånger större* än vad de är i dag, för att individer som behandlats dåligt av en myndighet ska slippa bli betalningsskyldiga vid upprättelsen.

---

66 SOU 2015:23 Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten: ”*Utredningen menar att den av regeringen tidigare redovisade strategin (prop. 2001/02:158) liksom den i betänkandet SOU 2005:42 föreslagna i grunden var riktiga. Utredningen anser dock att de båda har sökt åtgärda samtliga problem och utmaningar i hela samhället i ett sammanhang, något som ställer genomföranden inför överväldigande utmaningar.*”

Då NISU-utredningen enligt Dataskydd.net:s bestämda åsikt missat att uppmärksamma till exempel Post- och telestyrelsens strategi (se fotnot 34), samt en längre rad andra strategier och praktiska råd utarbetade av IT-kommissionen, Datainspektionen och en rad andra myndigheter, upplevde Dataskydd.net förra året och alltjämt att det mest överväldigande var NISU-utredningens oförmåga att leta fram och utvärdera IT-säkerhetsstrategier.

67 Se ENISA, ”Security Economics and the Internal Market”, 2008:

> *Information security is now a mainstream political issue, and can no longer be considered the sole purview of technologists. Fortunately, information security economics has recently become a live research topic: as well as collecting data on what fails and how, security economists have discovered that systems often fail not for some technical reason, but because the incentives were wrong. An appropriate regulatory framework is just as important for protecting economic and other activity online as it is offline.*

Se även Dorothy Denning, ”Toward More Secure Software”, Communications of the ACM, april 2015, Vol. 58 Issue 4, p24-26:

> *Right now, companies are not liable, protected by their licensing agreements. No other industry enjoys such dispensation.*

Se även Jan Muntermann och Heiko Roßnagel, ”On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market”, i Identity and Privacy in the Internet Age, Volume 5838 of the series Lecture Notes in Computer Science, pp 1-14. Springer Berlin Heidelberg, 2009:

> *[T]he role of privacy breach disclosure regulations and the possible incentives such regulations might provide to invest in security measures represent a matter of increasing interest. /.../ Our results show that privacy incidents represent an event type the capital markets do significantly react to. However, compared to other event types, the observed price reactions show an effect magnitude that question the effectiveness of corresponding regulations concerning their stimulus to invest in security measures.*

68 Man kan på sannolika grunder anta att detta är en anledning till att försäkringsindustrin aldrig nått stora framgångar med att försäkringsvägen incentivera större investeringar i informationssäkerhet. För en genomgång av de ekonomiska faktorer som gör försäkringsmodellen osäker i just informationssäkerhetssammanhang *se till exempel* Rainer Böhme, Cyber-Insurance Revisited, WEIS 2005 *och* Rainer Böhme och Galina Schwarz, Modeling Cyber-Insurance: Towards A Unifying Framework, WEIS 2010. *Se även* ENISA, The cost of incidents affecting CIIs, 2016 *samt pressmeddelandet* ENISA, Determining the real economic impact of cyber-incidents: A mission (almost) impossible (10 augusti 2016):

> *Cyber security incidents affecting CIIs (Critical Information Infrastructures) are considered nowadays “global risks that can have significant negative impact for several countries or industries within the next 10 years”. But the job of identifying the real impact produced proves to be quite a challenge.*

Eller märk svårigheterna Myndigheten för samhällsskydd och beredskap hade att konkretisera skadeverkningarna av driftsstörningarna hos Tieto i ”Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011” (februari 2012).

kräva organisatoriska omställningar.[69] Kostnaden för mer betydande informationssäkerhetsuppgraderingar i vanligen använda infrastrukturer kan till och med uppfattas som så omfattande att man politiskt fattar beslut om att låta den privata sektorn undkomma investeringarna genom att falla tillbaka på lagstiftning,[70] och statliga utredningar och lagstiftning om informationssäkerhet bekräftar också att den stora utmaningen just är att hitta kostnadseffektiva sätt att skapa säker informationsinfrastruktur.[71] Det blir alltså i viss mån larvigt när svenska myndigheter som Riksrevisionen låtsas som att det som saknas för bättre informationssäkerhet är strategidokument och interna policys.[72]

Ett exempel på detta är de över 200 bedrägerier som drabbade Örebrobor i samband med beställningar från OnlinePizza.se våren 2016.[73] Problemet som drabbade de bedragna hade uppenbarligen en teknisk lösning (OnlinePizza.se ändrade sina rutiner för betalning efter att händelsen fått mediauppmärksamhet) men de drabbade agerade i första hand genom att polisanmäla. Först när polisen förtydligade i media att de inte kunde kompensera för de bristfälliga rutinerna tillkännagav företagen att de kunde förbättra sitt system. Till skillnad från myndigheter som Post- och telestyrelsen eller Konsumentverket kan polisen inte komma till rätta med företag som inte vill genomföra nödvändiga säkerhetsförbättringar på ett systematiskt sätt. Detta är symptomatiskt för säkerhetsfel i IT-system och förvärras av att säkerhetsfel bara åtgärdas efter storskaliga mediauppbåd. Hade de bedrägeridrabbade varit färre, till exempel tio personer i stället för 200, är det osannolikt att det här felet hade åtgärdats.

De höjda administrativa avgifterna som kan utdömas av Datainspektionen efter det att EU:s dataskyddsförordning träder i kraft i maj 2018 är inte tillräckliga. Ett förslag från utredningen att på informationssäkerhets- och dataskyddsområdet avvika från den etablerade svenska skadeståndsdoktrinen skulle ge enskilda individer ett kraftfullt verktyg att ställa organisationer till svars, och samtidigt ge organisationerna incitament att förbättra sig säkerhetsmässigt.

Möjlighet att påvisa att något gått fel

Integritetskommittén noterar att man *bara* behöver visa att det skett ett fel för att ha rätt till skadestånd.[74] Myndigheters och företags IT-system skyddas emellertid både av lagen om företagshemligheter, bestämmelsen om dataintrång i brottsbalken, och kan täckas av säkerhetsskydd. Därför kan det av

Juridiskt svårt och tekniskt lätt. De 200 pizza-bedrägerier som ägde rum i Örebro under våren 2016 är tekniskt lätta att lösa, men juridiskt svåra att lösa. Till exempel har polisen enligt uppgift i Nerikes allehanda inte kapacitet att kompensera för att det är tekniskt lätt att bedra en med-medborgare. Samtidigt vore det svårt att kräva att Klarna använder ett annat system för att bekräfta fakturamottagarens identitet än vad som i dag är fallet: skulle det ställas krav på e-legitimation skulle Klarna inte längre ha en konkurrensfördel mot banker, och betalning skulle bli besvärligt igen. En möjlig lösning vore att statliga myndigheter slutar sälja identitetsuppgifter om medborgare till företag som publicerar dem på nätet, men det förefaller också osannlikt. Tidigare och framtida offer för identitetsstöld och fakturabedrägeri har många år av stora besvär att se fram emot medan politikerna överväger hur de ska hantera dataskydd.

[69] För två exempel i närtid se Datainspektionen, beslut i tillsynsärende kring användning av hjälpmedelssystemet Sesam i Region Skåne, diarienummer 1863-2015 *samt* Förvaltningsrätten i Stockholms dom den 14 april 2016, mål nummer 8059-15. Den senare citerade domen bekräftar Datainspektionens tillsynsbeslut att rutinerna vid en viss vårdinstans för utdelning av tillgångsbehörighet i ett system för patientinformation behövde förändras. En sådan rutinförändring har stor inverkan på relationerna mellan chefer och anställda, samt de anställdas förutsättningar att använda de informationsteknologiska verktygen på de sätt som krävs för att deras vårdinstitution ska få betalt, klara sina administrativa förpliktelser och, i någon utsträckning, även ge vård på det sätt de kommit att bli vana vid att ge vård.

[70] Läs till exempel redogörelsen i Stephanie K Pell, Christopher Soghoian. ”Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy”, Harvard Journal of Law and Technology, Volume 28, Number 1 Fall 2014; *men se även* den till Europarådets rekommendation R 89 (9) om IT-relaterad brottslighet hörande slutrapporten från European Committee on Crime Problems.

[71] Se till exempel bedömningarna av kostnadseffektivitet och kostnader i SOU 2015:23 Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.

[72] Riksrevisionen. RIR 2014:23 Informationssäkerheten i den civila statsförvaltningen.

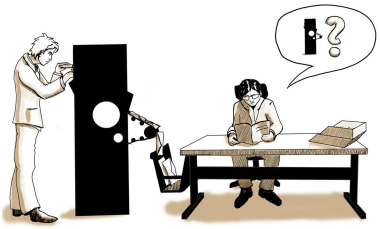
[73] Mattias Frödén, ”Härvan växer – hundratals offer för pizzabluffen”, Nerikes allehanda (23 april 2016).

[74] SOU 2016:41, s. 170.

praktiska skäl vara svårt för enskilda individer att faktiskt påvisa att det pågår en integritetskränkande eller dataskyddsstridig behandling av uppgifter.

Individcentrisk incidentrapporting som beskrivet ovan på sidan 7 skulle göra det lättare för enskilda individer att utkräva ansvar i alla fall vid säkerhetsmissar. Den på sidan 9 föreslagna sårbarhetsrapporteringen skulle också kunna utgöra ett verktyg för individer att utkräva ansvar för säkerhetsfel som är kända men som ännu inte lagats.

Regeringen skulle i sin *hållbart företagande*-verksamhet kunna utsträcka fokus från att bara röra företags verksamheter i utlandet,[75] till att även inkludera företags verksamheter inuti Sverige. Initiativ inom ramen för hållbart företagande skulle kunna innefatta dialoger med näringslivet om vikten av transparens kring dataskyddsrevisioner och att svenska företag för egen statistik över interaktioner med myndigheter (även svenska myndigheter) genom transparensrapporter. Det kan också vara lämpligt att uppmuntra företag att genomgå revisioner i stället för att förlita sig enkom på självskattningar.[76] Notera att detta ofta är väldigt dyrt för företag. Vad gäller myndigheter skulle de kunna öka transparensen kring mjukvarorna de använder och dessas funktioner (till exempel göra programkoden granskningsbar så att profilerande algoritmer kan undersökas, samt genom att följa rekommendationerna i utredningen om förbättrad samordning av offentlig IT-standardisering[77]). Specifika tekniska lösningar som *transparency logging* (se ovan sid. 12) finns – men det saknas ekonomiska incitament att använda dem, och bristen på efterfrågan skapar ett underskott på tillgänglig expertis.



Svarta lådan. ”Vad det här reflekterar är att vi har, under ett antal år nu, i ökande utsträckning levt bakom envägsspeglar, bakom vilka vi blir mer och mer transparenta för vår regering och även mot den privata sektorn, medan dessa blir allt mer ogenomträngliga för oss.” – Bart Gellman (Washington Post) vid Cato-institutets NSA Surveillance: What We Know; What to Do About It, 9 oktober 2013. [*transkribering och översättning: dataskydd.net*]

Bild av Markus Fridholm, CC-BY, december 2015.

Klagomål in abstracto och grupptalan

I Europadomstolen för mänskliga rättigheters praxis har det etablerats att man får överklaga en stats tillämpning av hemliga tvångsmedel utan att kunna påvisa att man själv blivit drabbad. Europadomstolen har resonerat att det ligger i de hemliga tvångsmedlens natur att enskilda personer som utsätts för tvångsmedlena inte kan veta om de är underställda sådan övervakning. Man kallar detta att det finns en rätt att överklaga *in abtracto*, som skiljer sig från normalfallet att man ska kunna påvisa att det skett en kränkning mot den egna

[75] *Se* UD 13.031 Hållbart företagande - Plattform för svenskt agerande.

[76] Se till exempel Chris Jay Hoofnagle, ”Assessing the Federal Trade Commission’s Privacy Assessments”, IEEE Security & Privacy Magazine; Mar 2016, Vol. 14 Issue 2, p58-64, 7p (2016). Han skriver:

> *The difference between audits and assessments is not popularly understood. Assessment is a term of art in accounting wherein a client defines the basis for the evaluation, and an accounting firm certifies compliance with the client-defined standard. An audit, on the other hand, is an evaluation against a defined, externally developed standard, such as an International Organization for Standardization (ISO) standard’s requirements. In assessments, an evaluator must only obtain “sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.” Pursuant to assessment rules, an assessor might rely on statements from the company regarding its privacy practices—that is, interview relevant employees—-rather than engage in testing. For instance, a company can claim that its scripts do not “respawn” cookies, and the assessor is permitted to accept that representation as true without further investigation.*

Man kan omedelbart uppskatta att det system som kodifierats i EU:s dataskyddsförordning inte ens förlitar sig på externa uppskattningar (till exempel utförda av en revisionsfirma), utan på att företag och myndigheter själva upprättar kriterier som de sedan själva får uppskatta om de följer.

[77] SOU 2007:47, Den osynliga infrastrukturen - om förbättrad samordning av offentlig IT-standardisering.

personen för att bli hörd av domstolen.[78]

Normalt ska tillsynsmyndigheterna genomföra representation av medborgarnas intressen *in abstracto*. På integritetsområdet kan det dock finnas skäl att utöka även medborgarnas egna möjligheter till självrepresentation. Det kan innefatta dataskyddsintrång som förvisso inte bevisligen drabbat den enskilda medborgaren (eftersom det ofta är mycket svårt att få bevisning på personlig åverkan), men som bevisligen drabbat någon som varit kund hos företaget eller hos myndigheten som den enskilda haft kontakt med.

I EU:s dataskyddsförordning finns inskrivet att individer ska kunna bli representerade av en organisation (till exempel en konsumentskyddsförening eller en dataskyddsförening) i rättsprocesser.[79] Ett liknande system finns i Sverige redan i dag på diskrimineringsområdet,[80] och man skulle kunna titta närmare på hur detta har fungerat i praktiken. En för Dataskydd.net ganska rimlig hypotes är att även ideella föreningar kommer att dra sig för att driva fall å enskilda privatpersoners vägnar om de därmed riskerar att behöva betala offentliga myndigheters rättegångskostnader.

Ett straffrättsligt skydd för rätten till dataskydd och rätten till integritet kan vara till sin natur svårt att tillämpa, eftersom straffrätten förutsätter att det finns en fysisk person som kan hållas straffrättsligt ansvarig. Olovlig databehandling sker dock ofta inom ramen för myndighets- eller företagsverksamhet. Oavsett svårigheten att utdöma straffrättsliga sanktioner, borde det dock vara så att de enskilda individer som drabbats av ett integritetsintrång får det lättare att begära skadestånd om det redan är visat att någonting har varit fel i en associations behandling av uppgifter.

Den bestämmelse i brottsbalken om olovligt integritetsintrång som justitieministern såg ut att försiktigt annonsera i somras[81] skulle kunna föreslås utökas till att omfattas även integritetsintrång som begåtts av myndigheter och företag. Frågan är vem som ska antas bära ansvaret.

Integritetskommittén kan överväga att liksom på immaterialrättens område ha en särskild åklagar- och polisenhet[82] som enligt reglerna om allmänt åtal agerar då de får kännedom om brott mot dataskyddslagstiftningen, i stället för å en enskild anmälares vägnar. Skillnaden borde vara att utvecklingen av praxis och doktrin i högre utsträckning kommer att behöva drivas framåt av myndigheterna själva, snarare än det presumtiva offret. Enskilda privatpersoner har sämre förutsättningar att anställda biträden och juridisk expertis än aktörer som utsätts för immaterialrättsintrång.

---

[78] Europeiska domstolen för mänskliga rättigheter. Roman Zakharov v. Russia ([GC], no. 47143/06, § 165, 4 december 2015:

> *[T]he Court has permitted general challenges to the relevant legislative regime in the sphere of secret surveillance in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them. In the case of Klass and Others v. Germany the Court held that an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him.*

[79] Artikel 80, förordning (EU) 2016/679.

[80] 6 kap 2 § diskrimineringslag (2008:567).

[81] Sveriges radio Ekot, Ny lag mot näthat kan börja gälla nästa år (25 juli 2016).

[82] Jfr *Nationella gruppen mot immaterialrättsbrott* och samordningen av polisutredningar på det immaterialrättsliga området som beskrivet i Rikspolisstyrelsens tillsynsrapport 2013:2 Polismyndigheternas handläggning av ärenden om immaterialrättsliga brott.

En dataskyddsombudsman skulle kunna hjälpa enskilda individer som drabbats av dataskyddsintrång, på samma sätt som diskrimineringsombudsmannen hjälper enskilda individer som drabbats av diskriminering. En fördel med att skapa en särskild funktion som har en mer reaktiv roll skulle kunna vara att enskilda individer som upplever sig ha utsatts för ett integritetsintrång inte behöver vänta på att Datainspektionens proaktiva avdelning uppskattar att den egna kränkningen blivit ett allmänintresse. Att ha en särskild funktion för att hantera individuella integritetskränkningar rimmar också väl med premissen att rätten till privatliv och rätten till dataskydd finns där för att skydda enskilda.

Utbildning av åklagare och domare i dataskyddsrätt

I utredningen om straffrättsligt skydd för integriteten[83] (straffskyddsutredningen) anförs att personuppgiftslagen inte kan utgöra ett tillräckligt verktyg för att skydda integriteten eftersom rättsväsendets aktörer upplever lagen är ”svårtillämpad” och att de har ”mycket dålig kunskap” om lagen.[84]

Detta är, som Dataskydd.net redan anmärkt i sitt remissyttrande till utredningen om straffrättsligt skydd för integriteten, ett problem eftersom utredningen på grund av rättsväsendets negativa inställning till dataskyddslagstiftningen inte anstränger sig för att lagstiftningen ska upprätthållas.

Det verkar rimligt att initiera *utbildningsinsatser* om det i dagsläget är så att integritetsskyddet uppfattas som tråkigt och svårt av de myndigheter som måste ta ett ansvar för att integritetsskyddet upprätthålls.

Att svenska jurister skulle ha uppfattningen att dataskydd är krångligt och svårtillämpat är inte svårt att förstå. Doktrinen har företrädevis fokuserat på att antalet registerförfattningar är stort samt förhållandet mellan den så kallade hanteringsprincipen (som de facto kommer bli gällande i Sverige i och med EU:s dataskyddsförordning) och missbruksprincipen (en princip som genomfördes i svensk rätt genom ändringar i personuppgiftslagen 2006 och som verkar ha sitt ursprung i amerikansk lagstiftning).[85] Rättspraxis och prejudikat saknas i hög utsträckning eftersom upprätthållande av dataskydd inte varit någon prioritet.

Som vi kommer att ta upp på sidan 23 är det också allt annat än enkelt att hänga med i integritetssvängarna. Att Integritetskommittén ska framställa förslag samtidigt som 16 utredningar, inom ungefär samma område men med helt eller delvis annorlunda målsättningar än Integritetskommittén, redan pågår borde vara en indikation på hur komplicerat lagstiftaren har gjort det både för de som ska implementera lagen (myndigheter och företag) och de som nominellt ska skyddas av den (konsumenter och enskilda).

Utbildningsinsatser. Dataskyddsdagen firas varje år den 28 januari i flera delar av världen (till exempel Europarådets upptagningsområde, eller i Australien). Den kan utgöra en bas för utbildningsaktiviteter även för det svenska juristväsendet, som i dagsläget ofta undanhåller sig närmare engagemang för dataskydd eftersom de ser lagen som svår att tolka och tillämpa.

Ekonomistyrning för myndigheter

Den ekonomiska styrningen av myndigheterna från Ekonomistyrningsverket är sådan att det kan vara svårt för myndigheterna att motivera ett gediget dataskydds- och datassäkerhetsarbete om det inte finns ekonomiska konsekvenser av att låta bli att ha ett gediget sådant arbete.

Detta märks inte minst på Riksrevisionens återkommande kritik mot myn-

[83] SOU 2016:7 Integritet och strfafskydd.

[84] Ibidem s. 273

[85] Dataskydd.net har bläddrat igenom masteruppsatser publicerade inom ramen för juridikprogrammen i Stockholm, Uppsala och Lund.

digheternas IT-säkerhetsarbete.[86]

Tittar man emellertid på hur regeringen och statliga utredare föreställt sig att de administrativa avgifterna i EU:s dataskyddsförordningen ska tillämpas,[87] ser det ut som att man snarare föreställer sig särskilda undantag för just myndigheter från administrativa sanktioner. I stället ska Datainspektionen i så hög utsträckning som möjligt samtala med tillsedda myndigheter om åtgärder, enligt en utredning om myndighetsdatalag som publicerades 2015.[88] En effekt av detta är att samma myndighet under mer än ett halv decennium kan agera lagstridigt utan att drabbas av konsekvenser.[89]

Samtidigt som man har en skarp begränsning av vilka ekonomiska åtgärder Datainspektionen kan sätta in mot myndigheterna påvisade Integritetskommittén att myndigheter (i innevarande fall ett landsting) som förlorar stämningar om dataskyddsintrång ändå kan få sina rättegångskostnader betalda av den enskilda individ som har kränkts (se ovan s. 15). Om risken för administrativa sanktionsavgifter i stället gjordes reell för myndigheter, och möjligheten för domstolarna att flytta rättegångskostnader till enskilda målsäganden reducerades, skulle detta kunna faktoriseras in i myndigheternas informationssäkerhetsbudget utan att Ekonomistyrningsverket kan uppfatta pengaallokeringen som flådig. Det kan i sin tur höja både (den tekniska) dataskyddsnivån och IT-säkerhetsnivån i myndigheternas verksamhet.

”Effektivisering” och IT-system

Begreppet ”effektivisering” i svenska statliga utredningar har ofta ställts i motsatsförhållande till dataskydd och personlig integritet. Integritetskommittén ser ut att ha gjort en ansträngning att bryta sig loss ur en sådan beskrivning, men har i stället landat i att dataskydd och integritet kan hamna i motsatsförhållande till ”potential”, ett enligt oss lika diffust och ohjälpsamt ord som inte förtydligar vilka målsättningar de offentliga verksamheterna har med IT-systemen. Varken effektivisering eller potential är objektiva begrepp, utan förhoppningsfyllda.

Ett mått på effektivisering i offentlig sektor vore att e-förvaltning hjälper myndigheten uppnå bättre *kostnadseffektivitet*. Kostnadseffektiviteten kan mätas i förhållande till statskassan (att verksamheten slukar så lite pengar så möjligt) eller i förhållandet till samhället i stort (att verksamheten ser till att kostnaden i kronor för samhället som helhet blir så liten som möjligt) eller i förhållande till en enskild (att det kostar så lite tid, pengar eller ansträngning som möjligt för en enskild att söka hjälp hos en myndighet). Dessa olika former

[86] RIR 2007:10 Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen, RIR 2014:23 Informationssäkerheten i den civila statsförvaltningen, RIR 2016:8 Informationssäkerhetsarbete på nio myndigheter.

[87] Kommittédirektiv 2016:15 Dataskyddsförordningen, Kommittédirektiv 2016:21 Genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet, Kommittédirektiv 2016:52 Dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde.

[88] SOU 2015:39 Myndighetsdatalag.

[89] Datainspektionen, Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, Dnr 2331-2015, 25 oktober 2016.

> *FRA har i många sammanhang ett behov av att registrera och behandla känsliga personuppgifter. Samtidigt måste även i denna verksamhet restriktivitet iakttas i fråga om att behandla sådana uppgifter vilket följer av kravet på absolut i nödvändighet i 1 kap. 11 § FRA-PuL. Datainspektionen förordade i sin rapport från 2010 en teknisk funktion för att säkerställa att den avvägning som gjorts när det gäller nödvändighetsbedömning dokumenteras i systemen. Någon sådan funktion har inte införts.*

av kostnadseffektivitet kan inte nödvändigtvis genomföras på samma sätt, och betyder inte samma sak, och kan hamna i konflikt med varandra.

Riksrevisionen har efterfrågat mer och enklare datadelning mellan myndigheter för att förebygga att tjänstemän beter sig felaktigt.[90] Detta kan minska mängden pengar en enskild verksamhet slukar eller öka dess kostnader för framställning av och förvaltning av uppgifter. Det betyder inte nödvändigtvis att den globala samhällsnyttan blir högre eller att det blir enklare för enskilda att söka hjälp hos myndigheten. På ett för effektiviseringssökande åtgärder typiskt sätt ger Riksrevisionens rapport inga indikationer på hur stora problem och kostnader de uppfattar att de bedrägliga statsanställda orsakar i frånvaron av ytterligare kontrollåtgärder.

Även om man bortser från kostnaderna för IT-säkerhet kan det vara dyrt för enstaka verksamheter att införa administrativa kontrollåtgärder även om dessa är datoriserade. Datorer är nämligen bra på att lösa problem som kräver stora mängder data och många beräkningar, men datan behöver komma någonstans ifrån. Till exempel tog regeringen i september 2012 bort kravet på VAB-intyg för att minska den administrativa bördan på Försäkringskassan och för de föräldrar som behövde vara hemma med sjukt barn.[91] En delegation som tillsatts av regeringen under sommaren 2016 för att se över bidragsfusk kommer förhoppningsvis att ta sig tiden att se efter om besparingarna till följd av minskad administration översteg den något högre nivå av VAB-fusk som säkert resulterade.[92]

En annan måttstock för effektivisering är *produktivitetsförbättringar*. Då skulle vi förvänta oss att personalbehovet gått ned i takt med att investeringarna i e-förvaltning ökar. Det senaste decenniet har antalet anställda i svensk offentlig förvaltning på statlig nivå har i stället gått upp i förhållande till befolkningsmängden. Mängden anställda i kommunal sektor och i landsting ser ut att ha gått ned, men det är svårare att se att detta skulle ha att göra med digitalisering och inte till exempel *outsourcing* eller något annat.

Det ökade behovet av personal kan ha att göra med att de statliga myndigheterna *gör fler saker* till följd av e-förvaltning än vad de gjort tidigare. Kausala samband mellan investeringar i e-förvaltning och produktivitetsförbättringar har inte undersökts, och Riksrevisionens granskning av statens digitaliseringsåtgärder lyckades inte hitta en bättre måttstock för effektiviseringar än effektiviseringen som sådan.[93]

I ett av Riksrevisionens särskilda fokusområden, den statliga e-tjänsten Mina meddelanden, finns det anledning att ifrågasätta *vems* produktivitet förvaltningen har försökt öka och på *vems* bekostnad. Riksrevisionen kritiserar att tjänsten inte har så många användare trots att man lagt 347 kronor på tjänsten per mottagare, men observerar inte att de flesta medborgare har ett begränsat intresse av omfattande kontakter med myndigheter. När man vill åstadkomma effektiviseringar är det viktigt att först bena ut vems produktivitet och kostnader

[90] Riksrevisionen. RIR 2010:18 Informationsutbyte mellan myndigheter med ansvar för trygghetssystem.

[91] Svenska dagbladet, Regeringen slopar krav på vab-intyg (17 september 2012).

[92] Kommittédirektiv 2016:60 En delegation mot överutnyttjande av och felaktiga utbetalningar från välfärdssystemen.

[93] Riksrevisionen. RIR 2016:14 Den offentliga förvaltningens digitalisering – En enklare, öppnare och effektivare förvaltning?.

TIPS
Innan man eftersätter informationssäkerhet och dataskydd för kontrollåtgärders skull, bör man utreda om de ytterligare kostnaderna för kontrollåtgärder kompenseras av den förväntade minskningen i bedrägligt beteende. Först när man har etablerat att de gör det, är det värt att gå vidare och ta reda på om de kontrollåtgärderna även är värda minskningen av informationssäkerhet och dataskydd som följer.

Ansvarsförskjutning. För de flesta medborgare är kontakter med myndigheter ett nödvändigt ont som man vill begränsa omfånget av. Om kontakterna med myndigheter är så omfattande att en tjänst som Mina meddelanden kan öka produktiviteten hos en medborgare har medborgaren sannolikt så många andra problem att dess liv ändå inte är särskilt tillfredsställande. Om man i stället är en produktiv medborgare så vill man sannolikt inte själv tvingas ta på sig ansvaret att skaffa ett extra elektroniskt verktyg (e-legitimationen) för att få komma åt kommunikationer från myndigheter.

En möjlig lösning på detta som tillämpats i Danmark och som för närvarande är föremål för utredning i Sverige är att helt enkelt tvinga medborgarna att använda den digitala brevlådan. Ett sådant tvång kan hjälpa till att motivera kostnaderna för att utveckla den här sortens digitala tjänster, men det är också ett tvång man inte ska fatta beslut om annat än med medvetenheten om att man prioriterat myndigheternas bekvämlighet över medborgarnas. I Sverige skulle man så klart också få problemet att medborgarna vid ett sådant tvång skulle drabbas av det ytterligare tvånget att sluta avtal med en e-legitimationsleverantör av något slag (i praktiken en bank).

man försöker minska, och om de åtgärder man väljer för att uppnå det målet riskerar att ålägga någon annan, till exempel en privatperson, det ansvar som myndigheterna tidigare hade. Tendensen att använda e-förvaltning som ett sätt att flytta ansvaret för förvaltningen av medborgarna från förvaltningen som sådan till medborgaren själv har observerats av Gabriella Jansson.[94] Dataskydd.net har dock inte kommit över någon forskning kring hur pass utbredda sådana ansvarsförskjutningar är i förhållande till svensk statsförvaltning.

Risken med att tala om IT-stöd i offentlig verksamhet som en sorts ”potential” att uppnå ett mål (”effektivisering”) som inte är väldefinierat är dock att man låter investeringar i IT kompensera för att man inte tar tag i andra organisatoriska problem. Man skjuter över de organisatoriska problemen på medborgarna och kan, på grund av svårigheten i att ändra stora IT-system, göra problemen mer permanenta än de annars skulle vara. Ett IT-system kan inte kompensera för ett befintligt organisatoriskt problem eller skapa en ny organisation. Det kan inte ta bort den stora politiska och intellektuella ansträngning det innebär att ta reda på vad man vill och varför man i sådana fall vill det. Inte heller omintetgör IT-systemen den arbetsmarknadspolitiska omständigheten att det helt enkelt är politiskt lättast att använda just offentlig sektor som en sorts arbetslöshetsreglator.

Bestyrkande och förslag på kapitel 24

Bestyrkande av utredningens förslag.

Dataskydd.net stödjer att en sammanställning av förslag med inverkan på integriteten publiceras varje år.

Dataskydd.net anser att så väl lagförslag som promemorior och utredningar från departementsserien samt sådana översyner som vi anger nedan att regeringen genomför eller ämnar genomföra, utöver statliga utredningar, inkluderas i en sådan framställning. Eftersom utformningen av just informationssäkerhetsåtgärder inom den statliga förvaltningen nästan ofrånkomligen påverkar enskilda individers rätt till integritet och deras möjlighet att utnyttja sin rätt till dataskydd bör även initiativ på detta område inkluderas i sammanställningen.

Vidare behövs kontinuerliga kontroller av de åtgärder myndigheter vidtar för att profilera enskilda individer. Till exempel bör den sortens verksamhet som kommittén uppmärksammat i delbetänkandets kapitel 11.1 kunna tilldelas uppmärksamhet med större regelbundenhet än vad som är fallet.

Antalet förslag, pågående utredningar och lagändringar är i dag stort. En promemoria sammanställd av Justitiedepartementet 16 maj 2016[95] uppger

[94] Gabriella Jansson. En legitim (elektronisk) förvaltning? : Om IT-utveckling i kommunal förvaltning, doktorsavhandling, Linköpings universitet. 2013.

[95] Promemorian finns inte publicerad av regeringen på internet men har namnet *Redogörelse av åtgärder för att stärka den personliga integriteten*. Dataskydd.net har förvärvat en kopia genom en annan organisation som fått tag på promemorian efter en begäran om utlämning av offentlig handling.

att inte mindre än nio utredningar för närvarande är på gång, utöver Integritetskommittén som sådan.

Dessa är, enligt promemorian, dataskyddsutredningen (Ju 2016:04) (Ju/L6),[96] utredningen om genomförande av dataskyddsdirektivet (Ju 2016:06) (Ju/L4, m.fl.),[97] utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14) (Ju/L6),[98] mediagrundlagskommitténs (Ju 2014:17) uppdrag vad gäller den personliga integriteten på webbplatser med utgivningsbevis (Ju/L6),[99] utredningen om en myndighet med ett samlat ansvar för tillsyn över den personliga integriteten (Ju 2015:02) (Ju/Å),[100] en översyn av domstolsdatalagen (Ju/DOM),[101] ett kommande kommittédirektiv om att följa upp vilka effekter permanentningen av vissa bestämmelser om hemliga tvångsmedel haft på skyddet för den personliga integriteten (Ju/Å),[102] ett kommande kommittédirektiv, Stärkt integritet i Rättsmedicinalverkets verksamhet (Ju/Å),[103] samt en översyn av Tullverkets och Skatteverkets registerförfattningar på det brottsbekämpande området på Finansdepartementet.[104]

Under sommaren har dock regeringen tillsatt tre nya utredningar om hur integritetsskyddet ska se ut inom hälso- och sjukvårdsforskning samt hälso- och sjukvård i allmänhet,[105] två ytterligare utredningar om förändringar (eller en förhoppning om att undvika förändringar) i svensk förvaltning till följd av dataskyddsförordningens ikraftträdande 2018,[106] fyra nya utredningar om brottsbekämpande myndigheters personuppgiftshantering och relaterade frågor[107] samt en utredning om grundläggande teknisk infrastruktur för e-förvaltning.[108]

Sammanlagt pågår det alltså 19 samtidiga processer att utvärdera, bedöma, förändra, förbättra eller försvaga integritetsskyddet. Det är, för att låna ett begrepp från datalagringsutredningen, *sammantaget* en ohanterligt stor mängd utredningar som görs, och det är egentligen inte förvånande att två på varandra följande integritetskommittér har kommit fram till att skyddet för den personliga integriteten är svagt och att lagstiftaren trots goda intentioner inte uppnår

[96] Kommittédirektiv 2016:15 Dataskyddsförordningen.

[97] Kommittédirektiv 2016:21 Genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet.

[98] Kommittédirektiv 2015:125 Kameraövervakning – brottsbekämpning och integritetsskydd med tilläggsdirektiv och utökat uppdrag (kommittédirektiv 2016:54).

[99] Kommittédirektiv 2014:97 En kommitté på det tryck- och yttrandefrihetsrättsliga området.

[100] Kommittédirektiv 2014:164 En myndighet med ett samlat ansvar för tillsyn över den personliga integriteten.

[101] Ej ännu tillsatt, så vitt Dataskydd.net kunnat utröna.

[102] Ej ännu tillsatt, så vitt Dataskydd.net kunnat utröna.

[103] Kommittédirektiv 2016:75 Stärkt integritet i Rättsmedicinalverkets verksamhet.

[104] Enligt promemorian pågår arbetet för närvarande, men information har inte gjorts tillgänglig via regeringens vanliga vägar att publicera till exempel utredningsuppdrag och någon remissrunda har inte, så vitt Dataskydd.net kunnat ta reda på, initierats än så länge.

[105] Kommittédirektiv 2016:41 En ändamålsenlig reglering för biobanker, Kommittédirektiv 2016:45 Översyn av regelverken för forskningsetik och gränsområdet mellan klinisk forskning och hälso- och sjukvård, Kommittédirektiv 2016:65 Personuppgiftsbehandling på forskningsområdet.

[106] Kommittédirektiv 2016:52 Dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde, Kommittédirektiv 2016:63 Personuppgiftsbehandling inom utbildningsområdet.

[107] Kommittédirektiv 2016:20 Moderna regler om beslag och husrannsakan, Kommittédirektiv 2016:22 Genomförande av direktiv om användning av passageraruppgiftssamlingar, Kommittédirektiv 2016:36 Hemlig dataavläsning, Kommittédirektiv 2016:46 Tilläggsdirektiv till Utredningen om genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism (Ju 2014:26)

[108] Kommittédirektiv 2016:39 Effektiv styrning av nationella digitala tjänster i en samverkande förvaltning.

sina mål att säkerställa ett sådant skydd.[109]

Till dessa utredningar kommer utredningar som förvisso inte har som huvudsakligt syfte att begränsa eller påverka skyddet av den personliga integriteten men som ändå har som implicit (eller explicit) målsättning att göra undantag från skyddet av den personliga integriteten och enskildas individers möjlighet att utöva sin rätt till dataskydd för att uppnå något högre kollektivt syfte.[110]

I Integritetskommitténs delbetänkande kapitel 18 förekommer hänvisningar till inte mindre än 2826 sidor tidigare statliga utredningar om hemliga tvångsmedel sammanställda under de senaste 10 åren, samtidigt som det enda nya bidrag som görs i kapitlets omfattande 50 sidor text är två sidor om polisens informationsinhämtning på (det öppna) internet.[111] Det här är tyvärr vanligt, och mängden utredningssidor är så omfattande att personer som inte har som heltidssysselsättning att läsa dem alla lätt kan överväldigas. Effekten av de omfattande utredningarna är att staten, trots att den försöker hålla en hög nivå av transparens, i stället blir ogenomtränglig för att det inte går att arbeta sig igenom beslutsunderlagen i en tillräckligt snabb takt.

Mediagrundlagsutredningen är nu klar.[112] Vi välkomnar utredningens ambition att säkerställa en större roll för integritetsskyddet även i svensk tryckfrihetslagstiftning, men vi anser att utredningen gjort stora missar.

Personuppgiftsförsäljning vid flera statliga myndigheter[113] leder till nätpublicering av de kategorier av uppgifter som krävs för att utföra identitetsstölder och genomföra felaktiga fakturautställningar i annans namn. Identitetsstöld är ett växande problem och felaktiga fakturor är också ett växande problem.[114]

Även om regeringen har vidtagit åtgärder mot olovlig identitetsanvändning genom att införa en ny brottsrubricering med detta namn[115] är det svårt att föreställa sig att polisen kan kompensera för den informationssäkerhetsbrist som uppstår genom att myndigheterna säljer (eller för den delen alls lämnar ifrån sig) dessa mängder personuppgifter till privat sektor. Åtminstone en statlig utredning har till exempel observerat att alla felaktiga identitetsanvändningar utom SMS-lån som utfärdas i annans namn redan omfattades av straffrättsliga bestämmelser.[116] Ett starkt skydd för integriteten och privatpersoners informationssäkerhet kräver i stället att även identitetsuppgifter undantas från tryckfrihetsförordningens regler.

Särskilt om polisiära och militära inskränkningar av privatlivet

Integritetskommittén hittar stora risker för integritetsskyddet för enskilda vid polisens användning av personuppgifter, till exempel i samband med kartläggning på det (öppna) internet och mobiltömningar. Vid Riksrevisionens

[109] SOU 2007:22 Skyddet för den personliga integriteten - kartläggning och analys, SOU 2016:41 Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén.

[110] Kommittédirektiv 2015:95 Omreglering av spelmarknaden, Kommittédirektiv 2016:1 Arbetsmiljöregler för ett modernt arbetsliv, Kommittédirektiv 2016:29 Genomförande av EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem, med många fler.

[111] SOU 2016:41, kap. 18.7, s. 499-500.

[112] SOU 2016:58, Ändrade mediegrundlagar.

[113] Till dessa räknas Skatteverket, Bolagsverket och Trafikverket.

[114] *Se t. ex.* Riksdagen, Identitetsstöld och företagskapning! Svar på skriftlig fråga 2015/16:225.

[115] *Se* Proposition 2015/16:150 Straffrättsligt skydd mot olovlig identitetsanvändning.

[116] Kap. 10.2, SOU 2013:85, Stärkt straffrättsligt skydd för egendom.

granskning av Säkerhets- och integritetsnämnden[117] samt vid DFRI:s genomgång av Säkerhets- och integritetsnämndens (SIN) egna material sommaren 2015,[118] visade det sig att tillsynen inte fungerar bra. Datainspektionen, SIN och SIUN har därutöver enbart till uppdrag att kontrollera att de tre förstnämnda myndigheternas uppdrag genomförs i enlighet med lagstiftarens önskningar, inte att dessa tre myndigheters uppdrag som sådant utgör proportionerliga och strikt nödvändiga inskränkningar av integriteten. Tillsynsutredningen har dock lagt förslag som åtgärdar vissa av de innevarande tillsynsproblemen.[119]

Ett allvarligare problem rör polisens användning av så kallade *IMSI-catchers* med hänvisning till att *etern är fri*. En IMSI-catcher gör det möjligt för polisen att låtsas vara en basstation i det mobila kommunikationsnätet, och på det sättet plocka upp kommunikation från en mobiltelefon i närheten av den falska basstationen. Man kan se på det som en sorts identitetskapning – polisen använder en teknologi som lurar mobiltelefonen att den autenticerar mot någonting annat än vad som är fallet. Identitetskapningen är dock laglig så länge polisen kan få tillstånd att använda samma frekvensutrymmen som mobiloperatörerna använder.

IMSI-catcher-användning i Sverige har kartlagts av Markus Naarttijärvi vid Umeå universitet.[120] Problemet förefaller vara att resonemanget om att *etern är fri* gör att polisen inte behöver specifika tillstånd för sin tillämpning av tekniken. Det finns därför inga beslut som kan överklagas, och det är omöjligt för dem som har drabbats av polisens identitetskapningar att känna till eller bevisa att de har utsatts. Det är inte uppenbart vilken tillsynsmyndighet som är ansvarig, eller ens om just denna applicering av *etern är fri*-resonemanget är laglig under europeisk rätt. Enligt Naarttijärvi används dock teknologin flitigt.

Därutöver har svenska regeringen under ett antal år ägnat sig åt fantasifulla tolkningar av både EU-rättsliga och Europakonventionsrättsliga prejudikat. Om varje privatperson som tar sig för att läsa ett visst domstolsbeslut, till exempel datalagringsbeslutet från EU-domstolen av den 8 april 2014,[121] får intrycket av beslutet att det innebär en viss sak, men regeringen och svenska domstolar i stället konstruerar begreppet *sammantaget*[122] för att motivera varför domslutet inte innebär det man spontant tror, riskerar man att urholka rättsmedvetandet i befolkningen. Om rättsmedvetandet sjunker, det vill säga att det blir mindre uppenbart för privatpersoner vad som är rimliga och orimliga tolkningar av lagstiftningen och rättigheter, har det konsekvenser även bortanför personuppgiftslagen, registerförfattningarna och tvångsmedelsregleringen.

Det kan till exempel leda till att färre människor bibehåller det höga förtroendet för myndigheter på både statlig och lokal nivå som länge präglat Sverige.

[117] Riksrevisionen. RIR 2016:2, Tillsyn över brottsbekämpande myndigheter – En granskning av Säkerhets- och integritetsskyddsnämnden.

[118] *Se* Föreningen för digitala fri- och rättigheter, Remissvar SOU 2015:31 Datalagring och integritet, s. 7.

[119] SOU 2016:65, Ett samlat ansvar för tillsyn över den personliga integriteten, s. 166 och s. 175-176.

[120] Markus Naarttijärvi, Swedish police implementation of IMSI-catchers in a European law perspective, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.006

[121] Europeiska unionens domstol, Domslut i de förenade målen C-293/12 och C-594/12, EU:C:2014:238.

[122] Ds 2014:23, Datalagring, EU-rätten och svensk rätt *samt* Förvaltningsrätten i Stockholms dom den 13 oktober 2014, mål nummer 14891-14.

Det kan leda till att människor börjar ifrågasätta demokratiska värderingar och mänskliga rättigheter som statsbärande koncept.

Dataskydd.net har sett att Konkurrensverket i en uppsatstävling 2015 motiverar pris till en student som skrivit om korruption vid upphandlingar på följande sätt: ”*Uppsatsen behandlar ett mycket aktuellt ämne på ett bra och strukturerat sätt.*”[123] Enligt det vinnande bidraget har området inte givits särskild uppmärksamhet tidigare.[124] Det finns anledning att fråga sig varför det här ämnet har börjat uppfattas som särskilt aktuellt, och om aktualiteten påverkas av en förtroendeskadande åtgärder som vidtas även utanför upphandlingsförfaranden.

Med största insikt om att beredskapen – i både den politiska kåren och i de underställda operativa verksamheterna – att tänka igenom sina krav och beslut ur rättsmedvetandesynpunkt inte nödvändigtvis behöver vara utpräglad, känner vi ändå att ett utelämnande av denna oro i det här svaret vore att göra vår analys orättvisa.

Särskilt om tekniska integritetsåtgärder

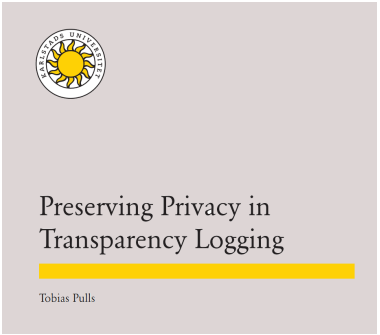
Nedanstående stycken upprepar observationer om tekniska integritetsåtgärder som vi redan har framför till andra utredningar, företrädevis i inlagor till pågående utredningar. Notera att Dataskydd.net inte menar att man behöver lagstiftande åtgärder för att införa dessa tekniska skyddsåtgärder för integriteten, utan att det som behövs är ett helhetsgrepp även i de delar av förvaltningen som ansvarar för upphandlingar av IT-system och myndigheternas organisering. En möjlig roll för det politiska (folkvalda) skiktet av individer i den statliga förvaltningen att spela i förhållande till dessa ”tips” är att ge dem uppmärksamhet, och se över möjligheten att skapa ekonomiskt utrymme för myndigheter att i högre utsträckning använda sig av dem.

Under hösten har Dataskydd.net bidragit till vissa av de pågående utredningarna som regeringen tillsatt om dataskyddsförordningens införlivande i svensk rätt. Där har vi gått igenom tekniska metoder och organisatoriska processer som kan tillämpas.

I viss utsträckning överlappar Dataskydd.net:s observationer med den vägledning för utredningar som Datainspektionen producerat[125] under hösten. Dataskydd.net har dock i högre utsträckning än Datainspektionen fokuserat på enskilda privatpersoners möjligheter att utöva sin rätt till dataskydd och privatliv, genom att föreslå åtgärder som kan göra både juridiken och tekniken mer transparent. Vi vill här följa upp med några exempel:

Rättsmedicinalverket Rättsmedicinalverket har efterfrågat en egen registerförfattning bland annat för att de i dagsläget lämnar ut uppgifter över okrypterad e-post. Dataskydd.net har i detta läge rekommenderat den för Rättsmedicinalverket tillägnade utredningen att överväga om det inte behövs tekniska snarare än juridiska åtgärder mot detta.[126]

Transparensloggning I samband med nya rön från Karlstads universitets PriSec-



Transparensloggning. Loggning av hur data transporteras genom flera myndigheters olika tjänster och IT-system på ett integritetsskyddande sätt kan vara en möjlig väg framåt för att få bättre integritetsskydd och dessutom att klargöra myndigheternas förhållanden till varandra i olika beslutsprocesser. En doktorsavhandling avlagd vid Karlstads universitet 2015 innehåller både praktiska exempel på hur sådan loggning fungerar och en teoretisk grund för dess bidrag till integritetsskyddet för enskilda privatpersoner.

[123] Konkurrensverket, Pristagare i uppsatstävlingen (2015).
[124] Emma Olsson, *Upphandlingsrättsliga sanktioner vid korruption - Uteslutning som medel för att stävja korruption*, kap. 1.5.
[125] Datainspektionen. Vägledning för integritetsanalys, 3 oktober 2016.
[126] Dataskydd.net, Inlaga till utredningen om stärkt integritet i Rättsmedicinalverkets verksamhet.

grupp har vi föreslagit att flera utredningar, om än inte i lag men i alla fall i dialog med myndigheterna som utreds, bör undersöka transparensloggning som ett sätt att göra förvaltningen av medborgarna mer begriplig för medborgarna, och säkerheten och integritetsskyddet bättre.[127]

Inbyggt integritetsskydd Vi har också rekommenderat att myndigheternas personuppgiftsbehandling analyseras utifrån Datainspektionens checklista för inbyggt integritetsskydd från 2012. Även om Datainspektionen inte i sin vägledning ser ut att ha tolkat dataskyddsförordningens artikel om inbyggt integritetsskydd som att detta vore nödvändigt menar vi att regeringens innevarande målsättning att stärka integritetsskyddet skulle gynnas av ett sådant angreppssätt.[128]

RFID Integritetskommittén har observerat att det inte uppstått så stora integritetsproblem kring RFID-tekniken som man till en början befarade.[129] Dataskydd.net vill tillfoga till denna observation att det bara finns ett exempel på framgångsrik standardisering av inbyggt integritetsskydd, som samtidigt fått stöd i både teori och praktik: Kommissionens rekommendation av den 12 maj 2009 om genomförandet av principerna om integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering (RFID) (2009/387/EG). Det kan vara lämpligt att begrunda om den genomtänkta och riktade insats som genomfördes för att säkerställa inbyggt integritetsskydd i RFID kan ha bidragit till att RFID inte blev något större problem.

E-leg och DNT: Standardisering som kantrat

Trots försök från EU-kommissionen att stödja integritetsvänliga lösningar för e-legitimation genom bland annat ett tvärvetenskapligt forskningsprojekt (FIDIS) och ett fortsättningsprojekt för standardisering av forskningsprojektets tekniska resultat (ABC4TRUST) har varken EU-kommissionens egna lagförslag (eIDAS-förordningen)[130] eller medlemsländernas satsningar (till exempel svensk e-legitimation) inkorporerat integritetsfrämjande resultat. I Sverige har Karlstads universitet deltagit i både FIDIS och ABC4TRUST genom sin PriSec-grupp, men utöver viss rådgivning till Datainspektionen har PriSec-gruppens breda kompetens inte kommit svenska beslutsfattare till gagn.[131]

http://FIDIS.net

https://abc4trust.eu

http://prisec.kau.se/

I andra standardiseringsprocesser, till exempel Do Not Track-gruppen[132]

[127] Dataskydd.net, Inlaga till utredningen om stärkt integritet i Rättsmedicinalverkets verksamhet *samt* Inlaga till utredningen om personuppgiftsbehandling inom utbildningsområdet *samt* Inlaga till utredningen om behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde *samt* Inlaga till utredningen om genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet.

[128] Se ovan 127.

[129] Kap. 12.3.4, SOU 2016:41.

[130] Kommissionens ursprungliga förslag till e-legitimationsförordning försökte i stället försvåra så kallad *anonym autenticering* eller *attributbaserad autenticering*. *Jfr* ABC4Trust One-Pager on eID Regulation:

> *[T]he current wording of the draft Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (COM/2012/238, hereinafter: eIDR) would hinder the deployment of advanced privacy features. It thereby fails its aim to be technology neutral. The eID Regulation also disregards the data minimisation principle. Besides this, the architecture logically following from the proposal requires one or more centralised national online authentication services which could profile their users' behaviour.*

[131] Notera att Dataskydd.net ovan lyfter vissa av PriSec-gruppens resultat.

[132] https://www.w3.org/TR/tracking-dnt/

på World Wide Web Consortium (W3C) vars syfte var att utveckla en teknisk metod för användare att signalera att de inte ville bli spårade samt en teknisk metod att säkerställa att denna preferens efterlevs av webbplatsförvaltarna, har representanter för europeiska tillsynsmyndigheter saknats. Detta trots att den europeiska lagstiftningen ställer krav som även i teknisk mening är förhållandevis specifika, och i större utsträckning än amerikansk lagstiftning kräver att marknadsaktörer frångår sina självupplevda ekonomiska intressen. En enda medarbetare från nederländska datainspektionen AP deltog i arbetsgruppen,[133] och EU-kommissionens engagemang var begränsat till ett antal offentliga yttranden från den dåvarande kommissionären. Gruppen har nu återupptagit sitt arbete.[134]

Randomiserade identifierare: standardisering som vore lämplig

I juni 2015 bestämde Datainspektionen att spårning av privatpersoners rörelsemönster i offentliga miljöer inte var förenligt med dataskyddsbestämmelser i svensk lag om privatpersonen inte uttryckligen godkänt sådan spårning innan den påbörjas.[135] Nederländska datainspektionen kom fram till en liknande slutsats i december 2015.[136] Samtidigt har vissa större teknikleverantörer, däribland Apple, experimenterat med ”randomiserade initiala identifierare” (i detta fall MAC-adresser).[137] Då sänder telefonen ut en slumpmässig MAC-adress som byts ut varje gång telefonen kopplar upp sig på nytt till accesspunkterna. Detta försvårar kartläggning av enskildas rörelsemönster. Detta uppmärksammas av Datainspektionen i deras tillsynsrapport, men Datainspektionen bedömer inte att denna teknik är tillräckligt utbredd för att utgöra ett effektivt skydd.

Här finns det utrymme för tydligare riktlinjer för hård- och mjukvarukomponenter i radioutrustning enligt EU:s direktiv 2014/53/EG om radioutrustning.[138] Som ett ”väsentligt krav” på radioutrustning omnämns[139] adekvat skydd för individers rätt till privatliv och dataskydd. Tyvärr upplever sig PTS enligt privat korrespondens med Dataskydd.net oförmögna att i egenskap av tillsynsmyndighet initiera dataskyddsstandardisering för radioutrustning, eftersom de menar att bara EU-kommissionen har rätt att initiera planering av föreskrifter. Datainspektionen upplever sig inte heller förmögna att agera på teknisk standardisering eftersom PTS är tillsynsmyndighet för radiolagen. EU-kommissionen upplever sig inte kunna agera då de säger sig vara beroende av att de nationella tillsynsmyndigheterna för upp möjligheten att standardisera och utfärda riktlinjer i den för syftet angivna arbetsgruppen.

Smarta elmätare: standardisering som struntar i dataskydd

I en utredning om funktionskrav på smarta elmätare[140] framställd av Energimarknadsinspektionen förra året lämnade Energimarknadsinspektionen all

[133] https://www.w3.org/2000/09/dbwg/details?group=49311&public=1
[134] *Se* https://www.w3.org/2016/11/tracking-protection-wg.html
[135] Datainspektionen. Besöksflödena i Västerås mäts för noggrant. 23 juni 2015.
[136] Autoriteit Persoonsgegevens. Wifi-tracking rond winkels in strijd met de wet. 1 december 2015.
[137] Se till exempel http://blog.mojonetworks.com/ios8-mac-randomgate/
[138] Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG.
[139] Ibid., artikel 3(3)(e).
[140] Energimarknadsinspektionen. Ei R2015:09, Funktionskrav på framtidens elmätare.

diskussion om dataskydd och IT-säkerhet därhän med hänvisning till att tillverkarna av smarta elmätare upplever att deras produkter redan är säkra. Både Post- och telestyrelsen[141] och Datainspektionen[142] påpekade att detta inte nödvändigtvis var givet.

Smarta elmätare är kända för att vara behäftade med ett stort antal dataskydds- och säkerhetsproblem:[143] dels är det möjligt att kartlägga individers beteenden i deras egna hem, och dels måste mätapparaturen kommunicera över flera protokoll och nivåer på ett sätt som är tekniskt svårt att säkra upp. Energimarknadsinspektionen hade också beställt en rapport från Umeå universitet som visade att smarta elmätare har mycket låga förutsättningar att få konsumenter att förändra sin energikonsumtion.[144] Detta beror på att konsumenter inte har möjligt att genomföra beteendeförändringar sådana att de får utslag på elräkningen i tillräckligt hög grad (besparingspotentialen ligger på ett fåtal kronor per flerfamiljshushåll). Inspektionen valde att tolka detta som att privatpersoner måste utsättas för mer granulär information om sitt beteende, i stället för att fråga sig varför man alls ska göra ingående mätningar av privatpersoners beteenden i sina egna hushåll om detta ändå har låga förutsättningar att bidra till en minskad elkonsumtion i hushållen.

I de här fallen är det svårt att se att ytterligare lagstiftning skulle vara hjälpsamt. Ett övergripande fokus i alla delar av den statliga förvaltningen på informationssäkerhet för både privatpersoner och för de verksamheter som använder teknologierna skulle dock kunna hjälpa.

Amelia Andersdotter
Ordförande, Dataskydd.net

[141] Post- och telestyrelsen, Dnr 15-6301. Yttrande över Energimarknadsinspektionens rapport Funktionskrav på framtidens elmätare (Ei R2015:09).

[142] Datainspektionen, Dnr 1045-2015. Energimarknadsinspektionens rapport Funktionskrav på framtidens elmätare (Ei R2015:09).

[143] *Se bl. a.* Ross Anderson och Shailendra Fuloria, Smart meter security: a survey, Cambridge University 2011.

[144] Thomas Broberg. Runar Brännlund. Andrius Kazukauskas. Lars Persson. Matthias Vesterberg, ”En elmarknad i förändring – Är kundernas flexibilitet till salu eller ens verklig?” Umeå universitet, augusti 2014. Rapport beställd av Energimarknadsinspektionen.

Källförteckning

Akademi och marknadsrapporter

1. ABC4Trust One-Pager on eID Reguation. https://ameliaandersdotter.eu/wp-content/uploads/2013/04/ABC4Trust-One-Pager-on-eID-Regulation-v1.0-for-publication-approval-and-distribution-at-ISO-workshop.pdf
2. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (2d ed. 2008). Tillgänglig gratis på internet: http://www.cl.cam.ac.uk/~rja14/book.html
3. Ross Anderson och Shailendra Fuloria, Smart meter security: a survey, Cambridge University 2011. https://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf
4. Axel M. Arnbak. ”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives” doktorsavhandling, Universiteit van Amsterdam, 2015. http://dare.uva.nl/record/1/492674
5. Malu Beijer, Blog seminar on positive obligations (3): Positive obligations to protect fundamental rights – any role to be played by the European Court of Justice?, Radboud University Nijmegen https://strasbourgobservers.com/2016/10/10/blog-seminar-on-positive-obligations-3-positive-obligations-to-protect-fundamental-rights-any-role-to-be-played-by-the-european-court-of-justice/
6. Thomas Broberg. Runar Brännlund. Andrius Kazukauskas. Lars Persson. Matthias Vesterberg, ”En elmarknad i förändring – Är kundernas flexibilitet till salu eller ens verklig?” Umeå universitet, augusti 2014. Rapport beställd av Energimarknadsinspektionen. http://ei.se/Documents/Publikationer/rapporter_och_pm/Rapporter%202014/Rapport_en_elmarknad_i_forandring_Umea_universitet.pdf
7. Rainer Böhme, Cyber-Insurance Revisited, WEIS 2005
8. Rainer Böhme och Galina Schwarz, Modeling Cyber-Insurance: Towards A Unifying Framework, WEIS 2010. http://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf
9. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI): Skrivelse till den pågående utredningen om hemlig dataavläsning. https://dataskydd.net/sites/default/files/dir201620_dfri_dataskydd_slutgiltig.pdf
10. Dataskydd.net, Inlaga till utredningen om genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet. https://dataskydd.net/sites/default/files/brottsbe_dataskydd_dir201621_inlaga_dataskyddnet.pdf
11. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI): Skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan. https://dataskydd.net/sites/default/files/dir201636_dfri_dataskyddnet_slutgiltig_2.pdf
12. Dataskydd.net, Inlaga till utredningen om personuppgiftsbehandling inom utbildningsområdet. https://dataskydd.net/sites/default/files/utbildning_dataskydd_dir201663_dataskyddnet_inlaga.pdf
13. Dataskydd.net, Inlaga till utredningen om behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde. https://dataskydd.net/sites/default/files/socialtjanst_dataskydd_dir201650_dataskyddnet_inlaga.pdf
14. Dataskydd.net, Inlaga till utredningen om stärkt integritet i Rättsmedicinalverkets verksamhet. https://dataskydd.net/sites/default/files/rmv_dataskydd_dir201675_dataskyddnet_inlaga.pdf
15. Deloitte, Deloitte Australian Privacy Index 2015: Transparency is opportunity. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-2015-090516.pdf
16. Dorothy Denning, Toward More Secure Software. Communications of the ACM, april 2015, Vol. 58 Issue 4, p24-26.
17. Joshua A. T. Fairfield och Christoph Engel, Privacy as a Public Good. Duke Law Journal, december 2015, Vol. 65 Issue 3, p385-457.

18. Fahriye Seda Gürses, Multilateral Privacy Requirements Analysis in Online Social Network Services, KU Leuven, 2010. https://www.cosic.esat.kuleuven.be/publications/thesis-177.pdf

19. Föreningen för digitala fri- och rättigheter, Remissvar SOU 2015:31 Datalagring och integritet. https://www.dfri.se/dfri/dfris-asikt-om/datalagringsdirektivet/remissvar-sou-201531-datalagring-och-integritet/

20. Gabriella Jansson. En legitim (elektronisk) förvaltning? : Om IT-utveckling i kommunal förvaltning, doktorsavhandling, Linköpings universitet. 2013. http://liu.diva-portal.org/smash/get/diva2:654083/FULLTEXT01.pdf

21. Jan Muntermann och Heiko Roßnagel, On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market, i Identity and Privacy in the Internet Age, Volume 5838 of the series Lecture Notes in Computer Science, pp 1-14. Springer Berlin Heidelberg, 2009.

22. Markus Naarttijärvi, Swedish police implementation of IMSI-catchers in a European law perspective, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.006

23. Helen Nissenbaum, Must Privacy Give Way to Use Regulation?, föreläsning på Brown University, 15 mars 2016. http://watson.brown.edu/events/2016/helen-nissenbaum-must-privacy-give-way-use-regulation

24. Emma Olsson, Upphandlingsrättsliga sanktioner vid korruption - Uteslutning som medel för att stävja korruption. http://www.konkurrensverket.se/globalassets/forskning/uppsatser/uppsats-2015_emma-olsson.pdf [åtkomst: 2016.11.03]

25. Stephanie K Pell, Christopher Soghoian. "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy" Harvard Journal of Law and Technology, Volume 28, Number 1 Fall 2014

26. Rachel M Peters, So you've been notified, now what? – The problem with current data breach notification laws, Arizona Law Review. 2014, Vol. 56 Issue 4, p1171-1202.

27. Tobias Pulls. "Preserving Privacy in Transparency Logging", doktorsavhandling, Karlstads universitet, 2015. http://www.diva-portal.org/smash/get/diva2:808057/FULLTEXT01.pdf

28. Sasha Romanosky, David Hoffman, Alessandro Acquisti, Empirical Analysis of Data Breach Litigation, WEIS 2012: http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf

29. Sasha Romanosky, David Hoffman, Alessandro Acquisti, Empirical Analysis of Data Breach Litigation. Journal of Empirical Legal Studies, 2014, volym 11(1), 74–104. http://onlinelibrary.wiley.com/doi/10.1111/jels.12035/abstract

30. Bruce Schneier, Data is a Toxic Asset, 4 mars 2016. https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html [åtkomst: 2016.11.03]

31. Steptoe & Johnson LLP, Comparison of US State and Federal Security Breach Notification Laws – Current through January 21, 2016. http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf [åtkomst: 2016.11.03]

Offentliga institutioner

1. Autoriteit Persoonsgegevens. Wifi-tracking rond winkels in strijd met de wet. 1 december 2015. https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-wifi-tracking-rond-winkels-strijd-met-de-wet

2. Datainspektionen. Besöksflödena i Västerås mäts för noggrant. 23 juni 2015. http://www.datainspektionen.se/press/nyheter/2015/besoksflodena-i-vasteras-mats-for-noggrant-/

3. Datainspektionen, Dnr 1045-2015. Energimarknadsinspektionens rapport Funktionskrav på framtidens elmätare (Ei R2015:09). http://www.regeringen.se/contentassets/696130de016b4d9598200df5ac6d454c/datainspektionen.pdf

4. Datainspektionen, beslut i tillsynsärende kring användning av hjälpmedelssystemet Sesam i Region Skåne, diarienummer 1863-2015 http://www.datainspektionen.se/Documents/beslut/2016-07-04-region-skane.pdf

5. Datainspektionen. Vägledning för integritetsanalys, 3 oktober 2016. http://www.datainspektionen.se/Documents/vagledning-integritetsanalys.pdf

6. Digitaliseringskommissionen, Temarapport 2016:1, Det datadrivna samhället. https://digitaliseringskommissionen.se/wp-content/uploads/2013/10/Temarapport-1_Det-datadrivna-samh%C3%A4llet-juni-2016.pdf

7. Ds 2014:23, Datalagring, EU-rätten och svensk rätt. http://www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2014/06/ds-201423/

8. Ds 2016:22 Polisens tillgång till information om vissa it-incidenter. http://www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2016/07/ds-201622/

9. Energimarknadsinspektionen. Ei R2015:09, Funktionskrav på framtidens elmätare. http://www.energimarknadsinspektionen.se/sv/Publikationer/Rapporter-och-PM/rapporter-2015/funktionskrav-pa-framtidens-elmatare-ei-r2015-09/

10. ENISA, Security, Economics and the Internal Market, 2008. https://www.enisa.europa.eu/publications/archive/economics-sec

11. ENISA, The cost of incidents affecting CIIs, 2016. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

12. ENISA (Press release), Determining the real economic impact of cyber-incidents: A mission (almost) impossible (10 augusti 2016). https://www.enisa.europa.eu/news/enisa-news/determining-the-real-economic-impact-of-cyber-incidents-a-mission-almost-impossible

13. Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation). http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32002L0058&qid=1465563881371&from=EN

14. Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG. http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32014L0053

15. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679&from=EN

16. Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF. http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016L0680&from=EN

17. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016L1148&from=EN

18. Europarådets rekommendation R 89 (9) om IT-relaterad brottslighet och den därtill hörande slutrapporten från European Committee on Crime Problems. ISBN: 92 – 871 – 1791 – 8. http://www.oas.org/juridico/english/89-9&final%20report.pdf

19. Europeiska konventionen för mänskliga rättigheter, ETS No.005. https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/005

20. Kommissionens rekommendation av den 12 maj 2009 om genomförandet av principerna om integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering (RFID) (2009/387/EG). http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32009H0387&from=EN

21. Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:sv:PDF

22. Kommittédirektiv 2014:97 En kommitté på det tryck- och yttrandefrihetsrättsliga området. http://www.regeringen.se/rattsdokument/kommittedirektiv/2014/06/dir.-201497/

23. Kommittédirektiv 2014:164 En myndighet med ett samlat ansvar för tillsyn över den personliga integriteten. http://www.regeringen.se/rattsdokument/kommittedirektiv/2014/12/dir.-2014164/

24. Kommittédirektiv 2015:95 Omreglering av spelmarknaden. http://www.regeringen.se/rattsdokument/kommittedirektiv/2015/09/dir.-201595/

25. Kommittédirektiv 2015:125 Kameraövervakning – brottsbekämpning och integritetsskydd. http://www.regeringen.se/rattsdokument/kommittedirektiv/2015/11/dir.-2015125/

26. Kommittédirektiv 2016:1 Arbetsmiljöregler för ett modernt arbetsliv. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/02/dir.-20161/

27. Kommittédirektiv 2016:15 Dataskyddsförordningen. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/02/dir.-201615/

28. Kommittédirektiv 2016:21 Genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/03/dir.-201621/

29. Kommittédirektiv 2016:29 Genomförande av EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/03/dir.-201629/

30. Kommittédirektiv 2016:39 Effektiv styrning av nationella digitala tjänster i en samverkande förvaltning. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/05/dir.-201639/

31. Kommittédirektiv 2016:41 En ändamålsenlig reglering för biobanker. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/05/dir.-201641/

32. Kommittédirektiv 2016:45 Översyn av regelverken för forskningsetik och gränsområdet mellan klinisk forskning och hälso- och sjukvård. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/06/dir.-201645/

33. Kommittédirektiv 2016:46 Tilläggsdirektiv till Utredningen om genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism (Ju 2014:26). http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/06/dir.-201646/

34. Kommittédirektiv 2016:52 Dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/06/dataskyddsforordningen--behandling-av-personuppgifter-och-anpassningar-av-forfattningar-inom-socialdepartementets-verksamhetsomrade/

35. Kommittédirektiv 2016:54 Tilläggsdirektiv till Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14). http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/06/dir.-201654/

36. Kommittédirektiv 2016:60 En delegation mot överutnyttjande av och felaktiga utbetalningar från välfärdssystemen. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/06/dir.-201660/

37. Kommittédirektiv 2016:63 Personuppgiftsbehandling inom utbildningsområdet. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/07/dir.201663/

38. Kommittédirektiv 2016:65 Personuppgiftsbehandling på forskningsområdet. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/07/dir.201665/

39. Kommittédirektiv 2016:75 Stärkt integritet i Rättsmedicinalverkets verksamhet. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/09/dir.-201675/

40. Konkurrensverket, Pristagare i uppsatstävlingen (2015). http://www.konkurrensverket.se/forskning/uppsatstavling/pristagare-i-uppsatstavlingen/ [åtkomst: 2016.10.21].

41. Konsumentverket, Rapport 2016:12 Digitalisering och konsumentintresset. http://publikationer.konsumentverket.se/sv/publikationer/rapporter/2016/rapport-2016-12-digitalisering-och-konsumentintresset.html?theme=classic [åtkomst: 2016.11.03]

42. National Conference of State Legislatures. Security Breach Notification Laws. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/7EDG-KVBF].

43. Post- och telestyrelsen. Strategi för ett säkrare Internet i Sverige. PTS-ER-2006:12.0 https://www.pts.se/sv/Dokument/Rapporter/Internet/2006/Strategi-for-ett-sakrare-Internet-i-Sverige---PTS-ER-200612/

44. Post- och telestyrelsen, Dnr 15-6301. Yttrande över Energimarknadsinspektionens rapport Funktionskrav på framtidens elmätare (Ei R2015:09). http://www.regeringen.se/contentassets/696130de016b4d9598200df5ac6d454c/post--och-telestyrelsen-pts.pdf

45. Promemorian Redogörelse av åtgärder för att stärka den personliga integriteten av den 16 maj 2016. Justitiedepartementet.

46. Proposition 2015/16:150 Straffrättsligt skydd mot olovlig identitetsanvändning. http://www.regeringen.se/rattsdokument/proposition/2016/03/prop.-201516150/

47. Proposition 2015/16:177 om fortsatt giltighet av tidsbegränsad bestämmelse i inhämtningslagen. http://www.regeringen.se/rattsdokument/proposition/2016/05/prop.-201516177/

48. Rikspolisstyrelsens tillsynsrapport 2013:2 Polismyndigheternas handläggning av ärenden om immaterialrättsliga brott. https://polisen.se/Global/www%20och%20Intrapolis/Tillsynsrapporter/2013/Tillsynsrapp_2_immaterialrattsliga_brott_130402.pdf

49. Riksrevisionen. RIR 2007:10 Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen. http://www.riksrevisionen.se/PageFiles/1174/RiR_2007_10.pdf

50. Riksrevisionen. RIR 2010:18 Informationsutbyte mellan myndigheter med ansvar för trygghetssystem. http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2010/Informationsutbyte-mellan-myndigheter-med-ansvar-for-trygghetssystem-/

51. Riksrevisionen. RIR 2014:23 Informationssäkerheten i den civila statsförvaltningen. http://www.riksrevisionen.se/PageFiles/20759/RIR_2014_23_infos%C3%A4kerhet_Anpassad.pdf

52. Riksrevisionen. RIR 2016:2, Tillsyn över brottsbekämpande myndigheter – En granskning av Säkerhets- och integritetsskyddsnämnden. http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2016/Tillsyn-over-brottsbekampande-myndigheter--En-granskning-av-Sakerhets--och-integritetsskyddsnamnden/

53. Riksrevisionen. RIR 2016:8 Informationssäkerhetsarbete på nio myndigheter. http://www.riksrevisionen.se/en/rapporter/Rapporter/EFF/2016/Informationssakerhetsarbete-pa-nio-myndigheter/

54. Riksrevisionen. RIR 2016:14 Den offentliga förvaltningens digitalisering – En enklare, öppnare och effektivare förvaltning?. http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2016/Den-offentliga-forvaltningens-digitalisering/

55. SOU 1976:69, Teknikupphandling. http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-7258406

56. SOU 2007:22 Skyddet för den personliga integriteten - kartläggning och analys. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/03/sou-200722/

57. SOU 2007:47, Den osynliga infrastrukturen - om förbättrad samordning av offentlig IT-standardisering. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/06/sou-200747/

58. SOU 2013:85, Stärkt straffrättsligt skydd för egendom. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/12/sou-201385/

59. SOU 2015:23 Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201523/

60. SOU 2015:31 Datalagring och integritet. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201531/

61. SOU 2015:39 Myndighetsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/

62. SOU 2016:7 Integritet och straffskydd. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/02/sou-20167/

63. SOU 2016:58, Ändrade mediegrundlagar. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/09/sou-201658/

64. SOU 2016:65, Ett samlat ansvar för tillsyn över den personliga integriteten. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/10/sou-201665/

65. Utrikesdepartementet. UD 13.031 Hållbart företagande - Plattform för svenskt agerande. http://www.regeringen.se/informationsmaterial/2013/11/ud-13.031/

Rättsfall

1. Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1.
2. Europeiska domstolen för mänskliga rättigheter. Roman Zakharov v. Russia ([GC], no. 47143/06, 4 december 2015.
3. Europeiska unionens domstol, Domslut i de förenade målen C-293/12 och C-594/12, EU:C:2014:238.
4. Förvaltningsrätten i Stockholms dom den 13 oktober 2014, mål nummer 14891-14.
5. Förvaltningsrätten i Stockholms dom den 14 april 2016, målnummer 8059-15.

Tidningsartiklar

1. Amelia Andersdotter, ”Innan vi petar i brottsbalken borde vi ta en förnyad titt på konsumenträtten”, Dagens juridik, 22 mars 2016. http://www.dagensjuridik.se/2016/03/debatt-idstold-amelia-andersdotter
2. Amelia Andersdotter, ”Hot mot personlig säkerhet och integritet - i Sverige räcker det med att vara folkbokförd”, Dagens juridik, 19 september 2016. http://www.dagensjuridik.se/2016/09/amelia-andersdotter-1
3. Amelia Andersdotter, ”E-legitimationslösning för tvångsregistrerade - ett större förvaltningsrättsligt problem”, Dagens juridik, 24 oktober 2016. http://www.dagensjuridik.se/2016/10/debatt-amelia-andersdotter-2
4. Simon Camponello, EU:s nya datalagar är klara – miljardböter för it-företag som missköter sig, IDG (17 december 2015).
5. Mattias Frödén ”Härvan växer – hundratals offer för pizzabluffen”, Nerikes allehanda (23 april 2016).
6. Svenska dagbladet, Regeringen slopar krav på vab-intyg (17 september 2012).