dataskydd.net

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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Stockholm 2016-03-01

Inlaga till integritetsutredningen Ju 2014:09

Innehåll

Inledning

Dataskydd.net är en partipolitiskt oberoende ideell förening vars syfte är att verka för informerade beslut om lagstiftning och teknologi i enlighet med de grundläggande rättigheterna till dataskydd och personlig integritet.

Vår verksamhet är projektfinansierad. Vi har fokuserat på enkla tekniska åtgärder som organisationer kan vidta för att uppfylla dataskyddslagstiftningens ideologiska principer, till exempel genom att inte kartlägga privatpersoner utan deras kännedom och genom att ha som princip att alltid tänka igenom hur åtgärder som förvisso är tekniska möjliga påverkar individers möjlighet till självbestämmande i digitala miljöer. För närvarande är verksamheten avgränsad till hemsidor.

Om utredningens uppdrag fram till maj 2016

Det finns idag många kartläggningar av integritetskränkningar, och integritetskränkningar spänner över många juridiska områden. Utredningen har fått i uppdrag att presentera en kartläggning av integritetskränkningar och möjligheten att införa ett integritetsombud senast i april 2016. Nedan återges Dataskydd.net:s syn på integritetsombud, begreppet ”risk”, datasäkerhet vs dataskydd, diskriminering som dataskyddstema, och konsumenträtt som dataskyddstema.

Integritetsombud

Utredningen ska överlägga om det behövs ett integritetsombud. Denna överläggning ska ske samtidigt som en annan utredning ska etablera om det behövs en samordnande myndighet för integritetsfrågor. Dataskydd.net menar att man istället behöver stärka de myndigheter som redan har i uppdrag att skydda privatpersoner, till exempel Datainspektionen.

Risken med att införa nya myndigheter är att man istället för att stärka möjligheterna att tillse lagstiftningen som redan finns, skapar resurs- och kompetenskonflikter mellan de olika tillsynsverksamheterna. Eftersom mängden myndigheter som arbetar med dessa frågor redan är väldigt stor, och problemet för privatpersoner är att myndigheterna som arbetar för allmänhetens intressen (och inte det allmännas intresse) är underfinansierade och små, är det enligt Dataskydd.net tveksamt om ytterligare en underfinansierad myndighet kommer att hjälpa privatpersoner. Andra åtgärder, som att lämna öppet för många organisationer att representera individer enligt ovan eller ge fler resurser till befintliga myndigheter, borde ha en bättre effekt.

Idag ansvarar Datainspektionen, Post- och telestyrelsen, Försvarets radioanstalt, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap med flera tillsammans för IT-säkerhetsfrågor. Datainspektionen, Post- och telestyrelsen och Konsumentverket ansvarar för olika aspekter av privatpersoners och konsumenters rättigheter i digitala miljöer, men vad gäller skärningspunkten mellan säkerhet och dataskydd är också Myndigheten för samhällsskydd och beredskap aktiva och försöker tipsa privatpersoner om hur de kan skydda sig mot datasäkerhetsproblem[1] (till exempel att identitetsuppgifter sprids utan individens kontroll). I en uppsats från Uppsala universitet färdigställd våren

[1] https://www.dinsakerhet.se/

2015 påtalas också möjligheten för privatpersoner att vända sig till Allmänna reklamationsnämnden.[2]

Dataskydd.net förstår skillnaden mellan Datainspektionen, Post- och telestyrelsen och Konsumentverket å ena sidan, samt Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt och Säkerhetspolisen å andra sidan, som varandes att de tre förstnämnda har ett uttalat uppdrag att utvärdera frågeställningar utifrån individens intressen, medan de tre sistnämnda har ett uttalat uppdrag att utvärdera frågeställningar utifrån statens, eller ”det allmännas”, intresse. Detta märks till exempel på hur Myndigheten för samhällsskydd och beredskap valt att utforma sina säkerhetstips: säker identitetsinformation och anti-virusprogram hjälper privatpersoner att agera på ett sätt som är så effektivt för banker och myndigheter som möjligt. Vid en fråga om huruvida säkerhetsbestämmelser finns, som ger privatpersoner möjlighet att utkräva ansvar av företag som kringgår säkerhetsåtgärder (till exempel reklamblockerare eller skriptblockera) som installerats i deras webbläsare, gav Myndigheten för samhällsskydd och beredskap ett nekande svar (för mer om detta, se nedan).

I frågor som rör spridning av personuppgifter, säkerhetsfunktioner, och transparens överlappar inte nödvändigtvis individers och statens intressen.

I sitt remissvar till utredningen om en ny myndighetsdatalag har Dataskydd.net framhållit att det vore bra att införliva en ombudsmannafunktion på Datainspektionen, så att enskilda kan få hjälp med kränkningar av deras dataskydd på samma sätt som diskriminerade kan få hjälp av diskrimineringsombudsmannen idag.[3] Diskriminering och dataskydd är delvis överlappande områden, vilket utvecklas nedan.

EU:s nya lagstiftning om dataskydd som färdigställdes i december 2015 innehåller, precis som den svenska diskrimineringslagen, en bestämmelse om att privatpersoner ska ha en rätt att utse en organisation att representera dem i dataskyddsprocesser. Eftersom EU:s dataskyddsförordning redan kommer att bli lag i Sverige från och med 2018 krävs inga ytterligare handlingar eller regler från utredningen eller lagstiftaren. Av demokratiskt intresse för EU är dock att Sverige lämnar öppet för många typer av organisationer att representera privatpersoner i dataskyddsprocesser: de europeiska länder som saknar stabila, demokratiska regeringen har nämligen i dataskyddsförordningen möjlighet att införa begränsningar för vilken sorts organisation som får utmana den sittande regeringen. Här kan Sverige agera positiv demokratisk förebild genom att frångå de detaljerade krav på organisationer med möjlighet att representera privatpersoner som återges i diskrimineringslagen.

GDPR, Artikel 76.
6 kap. 2 § diskrimineringslag (2008:568.

Notera att frågan om ombudsmannafunktion också är under prövning av EU-domstolen i målet C-192/15, Rease.[4]

[2] Grön, Jennie. *Framtidens bok – från avtalat ägande till övervakat lån*. Examensarbete i civilrätt. Juridiska fakulteten, Uppsala universitet, 2015. Tillgänglig på http://uu.diva-portal.org/smash/get/diva2:811095/FULLTEXT04.pdf

[3] Dataskydd.net, remissyttrande över SOU 2015:39, s. 25, 34. Tillgänglig på: https://dataskydd.net/sites/default/files/sou201539_remissyttrande_dataskyddnet.pdf

[4] EULawRadar, Case C-192/15, Rease – secretly spied on, medical data leaked, and left unprotected by the Dutch regulator. 1 maj 2015.http://eulawradar.com/case-c-19215-rease-secretly-spied-on-medical-data-leaked-and-left-unprotected-by-the-dutch-regulator/

”Riskbaserad bedömning”

Dataskydd.net föreslår att utredningen frångår begreppet ”risk” för beskrivning av integritetskränkningar. Riskbegreppet förutsätter att någon annan än privatpersonen (till exempel en myndighet eller ett företag) har rätt att fatta beslut om och kring privatpersonens uppfattning om vad som är bäst för privatpersonen, vilket går emot Europadomstolens praxis om privatliv och dataskydd som ett sätt att värna den individuella autonomin och identiteten (självbestämmandet). Riskbedömningar är därutöver någonting man gör när man utreder vilka säkerhetsåtgärder man ska installera i ett IT-system. Riskbedömningar inte lämpliga när man utreder i vilken utsträckning medborgare ska kunna utöva sina grundläggande mänskliga rättigheter.[5]

I konsumentskyddslagstiftning pratar man snarare om saker som kan vara ”oklara” för konsumenter i förhållande till tillgänglig information.

Exempel på sådana oklarheter i integritetsfrågor är vem en individ har relationer till. Vid ett testbesök på DN:s hemsida som Dataskydd.net har genomfört i februari etablerade DN kontakt med mer än 400 olika domäner åt användaren. Även om alla dessa domäner inte är unika företag, är det fortfarande betydligt fler företag man ställs i kontakt med än det enda företag man som webbesökare förväntat sig besöka. Andra oklarheter kan röra potentiella och realiserade datasäkerhetsrisker, till exempel om en myndighet eller ett företag läckt uppgifter eller inte har vidtagit sådana organisatoriska och tekniska åtgärder som man som konsument rimligen kan förvänta sig.

Integritetsutredningen har privilegiet att definiera på vilket sätt politiska ledare i Sverige kommer att förhålla sig till integritetsfrågor och dataskydd. Skillnaden mellan att beskriva individen som utsatt (för en risk) och att beskriva individen som varandes i dålig ställning att få klarhet (i en viss omständighet), är att den första beskrivningen gör individen passiv medan den andra skapar en bild av att individen bör ställas i bättre ställning att få klarhet och därför också ställas i bättre ställning att utöva sina rättigheter.

Datasäkerhet eller dataskydd?

Dataskydd.net har märkt att svenska utredningar saknar en bra distinktion mellan datasäkerhet och dataskydd. Därför föreslår Dataskydd.net följande distinktion: datasäkerhet är när ett system fungerar som det är tänkt. Det är möjligt att ha ett säkert system som ändå kränker individens rätt till privatliv och dataskydd. Dataskydd är att ett system fungerar på ett sådant sätt att individens rättigheter respekteras. Ett dataskyddande system måste vara säkert, men ett säkert system måste inte vara dataskyddande.

För en mer omfattande analys av olika begrepp som används för att beskriva dataskydd, datasäkerhet, individuell säkerhet, säkerhetsekonomiska modeller och institutionell säkerhet hänvisas till Axel Arnbaks avhandling vid Amsterdams universitet om de juridiska förutsättningarna för marknadsincitament för säker kommunikation för privatpersoner.[6] Arnbak har framför allt studerat

[5] Se Artikel 29-gruppens ordförande Isabelle Falque-Pierrotin i ett anförande inför franska nationalförsamlingen i december 2014. Sammanfattat på engelska, med länk till originalanförandet på franska, här: http://www.hldataprotection.com/2014/12/articles/international-eu-privacy/article-29-chief-criticizes-risk-based-approach/

[6] Arnbak, Axel M. *”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives”*, doktorsav-

hur Europa hanterar reglering av marknadsaktörer för krypteringscertifikat och elektroniska signaturer mot bakgrund av den nederländska certifikatutgivaren DigiNotars säkerhetsproblem 2010.

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). Han understryker att lagstiftaren ofta prioriterat *tillgänglighet* över *integritet* och *konfidentialitet*, samt att lagstiftaren upprepade gånger under de senaste årtiondena har bortsett ifrån kunskapen att åtgärder för att skydda slutkonsumenter stimulerar utvecklingen av bättre säkerhet i högre utsträckning än vad straffrätt gör. Arnbak lyfter också transparens för marknadens aktörer som en viktig utgångspunkt för konsumenter och stater att effektivt kunna lagstifta om, och upprätthålla lagstiftning om, datasäkerhet.

Profilering 1: Dataskydd och diskriminering

I ökat fokus för dataskyddsutredningar de senaste 10 åren är användningen av personuppgifter för att genomföra så kallad *profilering*. Profilering kan beskrivas som en uppdelning av individer i olika kategorier baserat på deras beteenden, beskaffenheter, vänskapskretsar eller bakgrund. Ofta genomförs profilering i marknadsföringssyfte. Det kan till exempel röra att man vill förutse vilken konsumentgrupp som kan antas vara mest intresserad av att ta emot reklam om en viss produkt. Det finns mycket litteratur om profilering, men av särskilt intresse är resultaten från det europeiska, tvärvetenskapliga forskningsprojektet FIDIS om identitet i informationssamhället. Boken *Profiling the European Citizen* gör en grundlig genomgång av juridiken kring dataskydd, diskriminering och den tekniska utvecklingen.[7] Detta arbete fortsätter inom ramen för EU-projektet A4CLOUD, som likt FIDIS har en tvärvetenskaplig inriktning som även innefattar tekniska aspekter.

http://FIDIS.net

http://www.a4cloud.eu/

Vidare är den nederländske juristen Frederik Zuiderveen Borgesius avhandling om integritetsskydd vid beteenderiktad reklam intressant, eftersom Borgesius anför att dataskyddslagstiftning inte är tillräckligt för att uppnå ett adekvat skydd mot den sorts kategoriserande åtgärder som man kan anta ligger konsumenter till last.[8] Även Federal Trade Commissions (FTC) rapport om *big data* och diskrimineringslagstiftning i USA kan vara upplysande, eftersom FTC redan i ett antal tillfällen tillämpat amerikanska anti-diskrimineringslagar på stordatabehandlingar.[9]

Profilering 2: Dataskydd och nudging

Profilering kan användas för så kallad *nudging*, en politisk metod för att få irrationella människor att bete sig mer rationellt (till exempel jogga mer, äta mindre socker, dela på föräldraförsäkringen) utan att aktivt interagera med

handling, Universiteit van Amsterdam, 2015. Tillgänglig på http://dare.uva.nl/record/1/492674

[7] Hildebrandt, Mireille, Gutwirth, Serge (red.). *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Springer Verlag, 2008

[8] Zuiderveen Borgesius, Frederik J., *Improving privacy protection in the area of behavioural targeting*, doktorsavhandling, Universiteit van Amsterdam, 2014. Tillgänglig på http://dare.uva.nl/record/1/434236

[9] Federal Trade Commission, 2016. *Big Data: A Tool for Inclusion or Exclusion?* Tillgänglig på: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

individen om att man vill att de ska genomföra dessa beteendeförändringar (genom till exempel politisk propaganda eller lagstiftning). *Nudging* beskrevs initialt av de amerikanska ekonomerna Cass Sunstein och Richard Thaler som en metod att använda mjuka styrningsmetoder för att få individer att anpassa sig efter ett policy-mässigt önskvärt beteende.

I Europa har *nudging* använts framför allt i Storbritannien. Den brittiska regeringen har en *nudge*-enhet vars uppdrag bland annat innefattar att övertyga människor om att myndigheter gör bra saker. Det europeiska forskningsprojektet D-CENT har studerat på vilka sätt identiter används som transaktionsmedel och i vilken utsträckning det används för att utöva påtryckningar mot individer av politiska skäl.

http://dcentproject.eu/

Svensk förvaltning har också *nudging*-projekt, till exempel i den kontroversiella frågan om föräldraförsäkring. Efter att politikerna under många år misslyckats att komma överens om huruvida man ska tvinga föräldrar att dela lika på föräldraförsäkringen har man infört ett mer subtilt system med ekonomiska incitament där duktiga föräldrar som delar lika får ett ekonomiskt bidrag, medan dåliga föräldrar som inte delar lika inte får något ekonomiskt bidrag.[10] Man har flyttat diskussionen från en öppen arena där varje medborgare själv kan ta ställning till hur den uppfattar de olika politiska föreställningarna om föräldrars skyldigheter och rättigheter, till en sluten arena som är svår för varje enskild medborgare att ta till sig - inklusive när denna medborgare befinner sig i situation att den gynnas eller missgynnas av bete sig på det ”önskvärda” sättet.

Evgeny Morozov är en amerikansk teknologikritiker som skrivit om hur profilering och *nudging* flyttar maktutövning från det offentliga till det slutna.[11] Morozov menar att den här tekniken för beslutsfattande om vad som ska vara *det goda livet* innebär manipulation, och att det förstör premisserna för det demokratiska beslutsfattandet. I Sverige utreds förhållandet mellan samhället, dess värderingar och teknikbeskrivningar främst vid Göteborgs universitet. Teknikhistoria kallas det idéhistoriska forskningsområde som framför allt bearbetat teknikens samverkan med samhällets värderingar. Två särskilda verk som Dataskydd.net vill lyfta fram är *The Government Machine* av den brittiske teknikhistorikern Jon Agar,[12] och resultatet av seminariet *Internet as common or capture of collective intelligence* som anordnades inom ramen för D-CENT-projektet.[13]

http://ait.gu.se/

Den sociala plattformen Facebook har genomfört politiskt relevant forskning på sina användare, och bland annat konstaterat att de kan förändra samhällssynen hos väldigt stora grupper människor genom att sortera nyheter och selektivt visa vissa postningar till vissa grupper. I en stor studie med runt 700000 (ofrivilliga och ovetande) deltagare visade man att människors känslotillstånd kan

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

[11] Morozov, Evgeny. The Real Privacy Problem. MIT Technology Review Magazine November/December 2013. Tillgänglig på http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/

[12] Agar, Jon. *The Government Machine: A Revolutionary History of the Computer* The MIT Press, 2003.

[13] D-CENT, Internet as common or capture of collective intelligence. 6 augusti 2015. Tillgänglig på: http://dcentproject.eu/wp-content/uploads/2015/08/D3.3-Annex-Internet-Identity-Seminar_annex.pdf

manipuleras med hjälp av mjuk styrning av den information de har tillgång i sina ”flöden”.[14] De individer som fått mer positiva budskap hade efter studien en mer optimistisk syn på utvecklingen framåt, medan den grupp som fått negativ information var betydligt mer pessimistisk. Här uppstår demokratiskt relevanta frågeställningar: vad händer om Facebook styr flöden inför allmänna val? Inför folkomröstningar? På vilka sätt skiljer sig denna sorts maktutövande från traditionella mediers maktutövande? En möjlig utgångsobservation är att de sociala plattformarna är mer personifierade och drar större nytta av människors relationer till varandra. Regeringens särskilt tillsatta mediautredare Anette Novak verkar ha närmat sig området genom hennes ifrågasättande av stora sökmotorers inverkan på individers informationstillgång. Även i EU har man diskuterat sökneutralitet, och begreppet finns tydligast beskrivet och utrett i franska Conseil d’Etats rapport om plattformsneutralitet från 2014.[15]

I praktiken går det inte heller att utföra studier på området utan att koppla sig till något av de stora sociala nätverken eller utan att vara en stat. Är man en fristående forskare är risken hög att man hamnar i konflikt med någon sorts industrirätt, till exempel företagshemligheter eller upphovsrätt. I både diskussionen kring profilering och *nudging* kan man observera att både stater och företag har starka intressen av att använda samma metoder, även om deras målsättningar kan skilja sig åt. För individen är det dock framför allt metoden att subtilt manipulera stora grupper människor som kan beskära friheten. Det gör att individens intressen kolliderar med både staters och företags intressen, och det finns få eller inga sätt för individen att hävda sig mot dessa två starka och sammanhållna intressegrupper.

Samhället har blivit likt ett ensidigt spegelglas: medan stater och företag trivialt kan hålla reda på hur en viss individ har känt sig vid exakta tidpunkter i det förflutna, och bestämma hur individen ska behandlas på bas av denna information, kommer individer ofta inte ihåg sina liv i sådan granulär upplösning. En positiv utveckling är att EU:s nya dataskyddslagstiftning inte längre strikt anger att industriella rättigheter är viktigare än individuella rättigheter, utan bara anger att industriella rättigheter normalt inte bör påverkas av att individer utövar sina rättigheter. Detta kan öppna för mer oberoende forskning kring hur individer påverkas, profileras och manipuleras av sina nätmiljöer.

Direktiv 95/46/EG, skäl 41, i jämförelse med GDPR, skäl 51.

Dataskydd och konsumenträtt

Vid Handelshögskolan i Stockholm har man studerat konsumenters, arbetstagares och aktieägares reaktioner på dåligt dataskydd.[16] En av slutsatserna är att konsumenter blir besvikna på ett företag som inte uppfyller deras dataskyddsförväntningar. Detta gäller även om företaget har skrivit in i sina slutanvändaravtal att de tänker göra på det sätt som upprörde konsumenten.

[14] Kramer, Guillory, Hancock. Experimental evidence of massive-scale emotional contagion through social networks. PNAS, 2014. Tillgänglig på: http://www.pnas.org/content/111/24/8788.full

[15] Conseil d’Etat. *Le numérique et les droits fondamentaux*. 2014. Tillgänglig på: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541/0000.pdf; se emellertid också Musiani, Francesca. *French Council of State: for a more ‘digitally-suited’ law?*, Policy Review, 13 oktober 2014. Tillgänglig på https://policyreview.info/articles/news/french-council-state-more-digitally-suited-law/327.

[16] ”Risker och riskhantering i näringsliv och samhälle”. Wahlund, R. (Red.) 2016. Stockholm School of Economics Institute for Research, Stockholm. (s. 95–).

Konsumenter godkänner väldigt många standardavtal på internet: en amerikansk studie uppskattar att det skulle ta runt 244 timmar per år att skumma alla avtal man formellt förväntas ha läst på internet under samma tidsperiod.[17] Att förstå innebörden av avtalen tar rimligen ännu längre tid.

Långa avtal som ger tjänsteleverantören få förpliktelser och konsumenten många förpliktelser är normalt på internet. Jennie Grön skriver i sin masteruppsats om framtidens bok:

> [D]en snabba standardiseringen av kontraktsvillkor kan skapa "negativa normer" för konsumenter. Konsumenter har ofta ingen möjlighet att gå till en annan näringsidkare inom samma näringsverksamhet för att få andra villkor, eftersom normeringen gjort att avtalsvillkoren i branschen är identiska. Valfriheten blir alltså illusorisk, eftersom inga reella alternativ existerar. När avtalsvillkoren blivit norm är det också mindre sannolikt att en domstol ser dem som oskäliga.[18]

Stora plattformar som Facebook och Twitter ålägger sig inga specifika förpliktelser gentemot konsumenter. I vissa fall är bevisbördan också omvänd till konsumentens nackdel: konsumenten måste kunna bevisa att den inte har gjort någonting, istället för att tjänsteleverantören ska kunna visa att konsumenten verkligen har gjort någonting.[19]

Här saknas samtidigt effektivt upprätthållande av dataskyddsregler, konsumenträttsregler och en balanserad syn på straffrätten som verktyg att lösa problem. Dataskydd.net vill ge tre specifika exempel:

- Riksdagen har under 2015 begärt att få olovlig identitetsanvändning kriminaliserad - ett förslag som regeringen under våren 2016 lovat att agera på.[20] Till grund för förslaget ligger en utredning från 2013 som menar att det huvudsakliga problem som ännu inte åtgärdats i lag kring identitetsanvändning är att individer tar ut SMS-lån i andra individers namn. Ingenstans under beslutsprocessen har någon frågat sig varför det är lätt att ta ut SMS-lån i andras namn, och om det inte är rimligt att finansiella organisationer säkerställer sig om att de lånar ut pengar till rätt person. Det är inte tekniskt omöjligt att se till att lån bara ges till sådana personer som faktiskt vill ha lån. Det är inte heller främmande för vårt juridiska system att se till att långivaren bär risken för att den lånat ut rätt mängd medel till rätt person.[21] Problemet verkar istället vara en föreställning om att vanliga regler inte gäller på internet, trots att de mycket väl skulle kunna göra det.

Bet. 2013/14:JuU15, rskr. 2013/14:159
Bet. 2014/15:JuU14, rskr. 2014/15:138

SOU 2013:85, Ett stärkt straffrättsligt skydd för egendom

[17] Aleecia M. McDonald och Lorrie Faith Cranor, I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue http://www.is-journal.org/ Tillgänglig på: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[18] Grön, Jennie. *Framtidens bok – från avtalat ägande till övervakat lån*. Examensarbete i civilrätt. Juridiska fakulteten, Uppsala universitet, 2015. Tillgänglig på http://uu.diva-portal.org/smash/get/diva2:811095/FULLTEXT04.pdf

[19] Litteraturen på detta område är mycket omfattande inom forskning på säkerhetsekonomiska modeller, men här är ett urval av texter som utredningen kan ha hjälp av: behandlingen av bevisbördesfrågor runt s. 106 i Lennart Johansson, "*Banker och internet*", Iustus förlag (Stockholm) 2006; Nicholas Bohm et al, "*Electronic Commerce: Who Carries the Risk of Fraud?*" 2000 (3) The Journal of Information, Law and Technology (JILT); Jean-Francois Blanchette, "*Burdens of Proof : Cryptographic Culture and Evidence Law in the Age of Electronic Documents*", MIT Press, 2012. För kortare läsning, se bl. a. https://www.lightbluetouchpaper.org/2010/02/11/chip-and-pin-is-broken/.

[20] Lagrådsremiss 11 februari 2016. http://www.regeringen.se/rattsdokument/lagradsremiss/2016/02/straffrattsligt-skydd-mot-olovlig-identitetsanvandning/

[21] Dataskydd.net. Skrivelse till riksdagen angående olovlig identitetsanvändning. 26 februari 2016. https://dataskydd.net/sites/default/files/olovlig_identitetsanvandning_dataskyddnet_20160225.pdf

- Inom dataskyddsforskningen och även dataskyddsaktivism finns ett ökat ifrågasättande av samtycke som juridisk bas för databehandling.[22] Det här ifrågasättandet har intensifierats under de senaste årens *big data*-diskussioner, liksom allt mer ifrågasättande av *ändamålsbegränsningen*, den juridiska princip som säger att man bara ska använda personuppgifter för det syfte de samlades in. Det finns dock också en stor samsyn kring att individens självbestämmande bör sättas i centrum, och att anledningen till att samtycke verkar praktiskt omöjligt är att självbestämmandet inte effektivt upprätthålls och skyddas av stater och tillsynsmyndigheter.[23] Att dra slutsatsen att en juridisk princip för samtycke är felaktig bara för att staten hittills inte skyddat denna rättighet för medborgarna är förhastat.

- Sveriges konsumenter anmälde i oktober 2014 biljettköpsleverantören Ticnet för oskäliga avtalsvillkor för ovarsam hantering av personuppgifter.[24] ”För att få köpa en biljett genom Ticnet måste du acceptera att de kartlägger dig och sprider dina uppgifter till andra företag runt om i världen – som då får laglig rätt att kontakta dig även om du är med i NIX. Samtidigt är det i många fall omöjligt att köpa biljetter till konserter och andra evenemang utan att gå genom Ticnet”, skriver organisationen. Våren 2015 indikerade ”generaldirektören och KO Gunnar Larsson [att] personlig integritet på internet ’kanske inte omedelbart en konsumentfråga.’”[25] Sedan dess har ingenting hänt. Jennie Grön indikerar att det trots flera möjligheter för konsumenter att kräva sin rätt i praktiken inte finns någon praxisutveckling.[26]

Det saknas regler som ger individer en möjlighet att uttrycka preferenser och skydda sina rättigheter på nätet. *Rätten* att uttrycka en preferens finns där, men inga europeiska myndigheter utom nederländska Autoriteit Persoongegevens har varit aktiva i att skapa en konkret *möjlighet* att utöva denna rättigheter (se nedan, om standardisering). Särskilt markndsföringsindustrin är aktiv i att ta fram tekniska metoder för att kringgå signaler från internetanvändare om att de inte vill ta emot skript, inte vill ta emot reklam eller inte vill bli spårade. Från en enskilds synvinkel utsätts man alltså dels för informationskampanjer om att man beter sig olojalt med internet, men man utsätts också för att de åtgärder man trots detta vidtar kringgås utan att man har någon möjlighet att skydda sig vidare, annat än genom att hoppas att skyddsmekanismerna utvecklar motståndskraft mot kringgående.

Dataskydd.net har via e-post framställt frågor till Myndigheten för samhällsskydd och beredskap, Datainspektionen, Post- och telestyrelsen samt Reklamombudsmannen om möjligheter för individer att utkräva ansvar av företag,

[22] Sinha, Amber, och Mason, Scott. *A Critique of Consent in Information Privacy* . Center for Internet and Society India, 11 januari 2016. http://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy

[23] Davies, Simon. *Why the idea of consent for data processing is becoming meaningless and dangerous.* Privacy Surgeon, 9 november 2015. Tillgänglig på http://www.privacysurgeon.org/blog/incision/why-the-idea-of-consent-for-data-processing-is-becoming-meaningless-and-dangerous/

[24] Sveriges konsumenter. Ticnet anmäls för oskäliga avtalsvillkor. 17 oktober 2014. http://www.sverigeskonsumenter.se/nyheter-press/pressmeddelanden/ticnet-anmals-for-oskaliga-avtalsvillkor/

[25] Jan Bertoft. Se upp för Blocket. 29 april 2015. http://bertoft.se/2015/04/se-upp-for-blocket/

[26] Grön, Jennie. *Framtidens bok – från avtalat ägande till övervakat lån.* Examensarbete i civilrätt. Juridiska fakulteten, Uppsala universitet, 2015. Tillgänglig på http://uu.diva-portal.org/smash/get/diva2:811095/FULLTEXT04.pdf

till exempel i marknadsföringsindustrin, som kringgår säkerhetsåtgärder som individen genomfört på sin egen dator eller i sin egen webbläsare, till exempel då marknadsföringsföretag via så kallade javascript kringgår insticksprogram i webbläsare som individer installerat för att slippa *malware* (skadlig kod) eller reklam.

Reklamombudsmannen svarade inom 24 timmar att ett sådant konsumentskydd saknas. Myndigheten för samhällsskydd och beredskap menade att IT-säkerhet för privatpersoner i just detta fall låg utanför deras normala verksamhetsområde, men att de inte hade kännedom om sådana regler. Datainspektionen menade att frågan inte låg på deras bord eftersom Post- och telestyrelsen har ansvar för sådana spårningsmetoder som reklamföretag använder i digitala miljöer. Post- och telestyrelsen menar att de bara har ett ansvar för en minskande mängd specifika tekniska spårningsåtgärder, men inte spårning generellt. Post- och telestyrelsen genomför för närvarande en tillsyn mot svenska hemsidor som använder sig av så kallade ”cookies” för att spåra användare, vars resultat väntades till vintern 2014 men som har dragit ut på tiden.

Särskilt om svenska utredningar om dataskydd och digitalisering

Dataskydd.net har, utöver den innevarande utredningen, arbetat med följande utredningar och förslag från det senaste året som påverkar den personliga integriteten:

- proposition 2014/15:148 om en ny domstolsdatalag,[27]
- proposition 2015:16/28 om vissa frågor om behandling av personuppgifter och regleringen av id-kortsverksamheten hos Skatteverket,[28]
- proposition 2015/16:65 om en ny utlänningsdatalag,[29]
- utredningen om informations- och cybersäkerhet i Sverige (SOU 2015:23),[30]
- utredningen om en ny säkerhetsskyddslag (SOU 2015:25),[31]
- utredningen om datalagring och integritet (SOU 2015:31),[32]
- utredningen om en ny myndighetsdatalag (SOU 2015:39),[33]

[27] Se Dataskydds.nets kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag. Skickat till Justitieutskottet. https://dataskydd.net/sites/default/files/domstolsdatalagen_kommentarer_dataskyddnet_ju.pdf

[28] Se Dataskydds.nets kommentarer till riksdagen om proposition 2015:16/28 om vissa frågor om behandling av personuppgifter och regleringen av id-kortsverksamheten hos Skatteverket. Skickat till Skatteutskottet, Konstitutionsutskottet, Justitieutskottet och Civilutskottet. https://dataskydd.net/sites/default/files/dataskyddnet_idregisterkommentar_sku.pdf

[29] Se Dataskydds.nets kommenterar på Proposition 2015/16:65 om en ny utlänningsdatalag. Skickat till Socialförsäkringsutskottet. https://dataskydd.net/sites/default/files/utlanningsdatalag_sfu_dataskyddnet.pdf

[30] Se Dataskydds.nets remissyttrande över SOU 2015:23 – Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. https://dataskydd.net/sites/default/files/sou201523_remissyttrande_dataskyddnet.pdf

[31] Se Dataskydds.nets remissyttrande över 2015:25 – En ny säkerhetsskyddslag. https://dataskydd.net/sites/default/files/sou201525_remissyttrande_dataskyddnet.pdf

[32] Se Dataskydds.nets remissyttrande över SOU 2015:31 – Datalagring och integritet. https://dataskydd.net/sites/default/files/dataskydd-dld-remiss.pdf

[33] Se Dataskydds.nets remissyttrande över SOU 2015:39 om en ny myndighetsdatalag. https://dataskydd.net/sites/default/files/sou201539_remissyttrande_dataskyddnet.pdf

- utredningen om personuppgiftsbehandling på utlännings- och medborgarskapsområdet (SOU 2015:73),[34] samt
- Energimarknadsinspektionens rapport om funktionskrav för smarta elmätare (Ei R2015:09).[35]

Därtill har Dataskydd.net arbetat med E-delegationens slutbetänkande.[36] E-delegationens slutbetänkande (SOU 2015:66) och samtliga andra skrifter från E-delegationen utgivna sedan 2009[37] tar inte upp dataskydd och integritet, trots att utredningsuppdraget specifikt klargjort att delegationen bland annat ska överväga hur medborgare kan utöva sina rättigheter. Vi har också arbetet med Digitaliseringskommissionens textsamlingar. Digitaliseringskommissionens tar precis som E-delegationen inte heller upp dataskydd och integritet.[38] I korrespondens med Dataskydd.net har Digitaliseringskommissionen angivit att detta är för att andra statliga verksamheter har ansvar för IT-säkerhet och dataskydd, men kommissionens förslag och inriktning har samtidigt långtgående konsekvenser för möjligheterna att bygga säkra och dataskyddande tekniska lösningar i både förvaltningen och i den privata sektorn.

SOU 2015:66.

Kommittédirektiv 2009:19, s. 8-9.

Till ovan listade utredningar kan läggas ytterligare utredningar om vården (SOU 2015:32), en passdatalagspromemoria (Ds 2015:44), en utredning om fakturabedrägerier (SOU 2015:77), och Post- och telestyrelsens arbete med samtyckesbegreppet i digitala miljöer. Därutöver har Dataskydd.net framför allt har varit aktiva under årets senare hälft, varför vi eventuellt missad viktiga utredningar som från årets tidigare hälft som egentligen borde tillfogas sammanställningen ovan.

Det måste stå klart att det inte är frågan om att integritetsfrågor inte utreds tillräckligt mycket i Sverige.

Däremot är det inte tydligt att de mänskliga rättigheterna genomsyrar förvaltningsarbete, lagstiftningsprocessen och investeringar i teknologi. Tidigare integritetsutredningar har observerat detta.[39] Observationen att det skett en förskjutning i åskådandet av rätten till privatliv som en samhälleligt relevant rättighet till att enbart vara en individuellt relevant rättighet har gjorts i doktrinen.[40] Det finns ingen anledning att tro att läget är förbättrat sedan integritetsutredningens slutsatser 2007, eller att den senast 2013 i doktrin beskrivna utvecklingen, på något sätt förändrats. Datainspektionen fann sig till exempel nödgade att göra ”principiella invändningar” mot utredningen om en ny myndighetsdatalag.[41]

SOU 2007:22, s. 445:
”*Om kvaliteten i lagstiftningen eftersätts får det en rad negativa konsekvenser. Det kan leda till att skyddsbehov av olika slag inte uppmärksammas eller får för liten uppmärksamhet i förhållande till andra intressen. Det kan också leda till att lagstiftningen blir osammanhängande, motsägelsefull och mindre väl förenlig med sitt syfte. Alla dessa slag av kvalitativa tillkortakommanden har kommittén påträffat vid sin kartläggning av den svenska integritetsskyddslagstiftningen. Även om denna lagstiftning på det stora hela är präglad av en ambition att tillgodose även skyddet för den personliga integriteten, finns det utan tvivel brister i såväl lagstiftningen som i sättet att utarbeta densamma.*”

[34] Se Dataskydds.nets remissyttrande över SOU 2015:73 om personuppgiftsbehandling på utlännings- och medborgarskapsområdet. https://dataskydd.net/sites/default/files/sou201573_remissyttrande_dataskyddnet.pdf

[35] Se Dataskydds.nets remissyttrande över Ei R2015:09 om funktionskrav på framtidens elmätare. https://dataskydd.net/sites/default/files/ei201509_dataskyddnet_remissyttrande.pdf

[36] Se Dataskydd.nets remissyttrande på SOU 2015:66 - E-delegationens slutbetänkande. https://dataskydd.net/sites/default/files/n2015_5090_ef_dataskydd_net_remissyttrande.pdf

[37] Se http://www.edelegationen.se/Publikationer/Betankanden/

[38] Se https://digitaliseringskommissionen.se/rapport/

[39] SOU 2007:22, Skyddet för den personliga integriteten - kartläggning och analys

[40] Naarttijärvi, Markus. Doktorsavhandling, Umeå universitet, 2013. “*För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*”.

[41] Datainspektionen. *Principiella invändningar mot ny myndighetsdatalag*. 26 november 2015.

Datainspektionens observationer om särskilt vårdverksamhet[42] och polisverksamhet[43] indikerar att lagstiftning, även när den tar vissa integritetsaspekter i beaktande, inte efterlevs.

Med hänvisning till sina tidigare skrivelser och remissyttranden, vill Dataskydd.net mena att det är en onödigt preskriptiv lagstiftning i kombination med bristfällig eller underfinansierad tillsyn och bristande intresse för dataskyddsfrågor från utredare på statliga departement och myndigheter som orsakar ett svårgenomträngligt och ihåligt skydd för den personliga integriteten.

Mer om komplicerad lagstiftning till dataskyddets nackdel

Som exempel kan anföras de nya reglerna om sökbegränsningar som införts i domstolsdatalagen, utlänningsdatalagen och ändringar i vissa förutsättningar för behandling av personuppgifter och regleringen av id-kortsverksamheten hos Skatteverket. Samtliga lagar innehåller en text som antingen är exakt, eller väldigt lik, den nedanstående:

> Vid sökning i personuppgifter är det förbjudet att som sökbegrepp använda uppgifter som avslöjar
>
> 1.ras eller etniskt ursprung,
>
> 2.politiska åsikter,
>
> 3.religiös eller filosofisk övertygelse,
>
> 4.medlemskap i fackförening,
>
> 5.hälsa,
>
> 6.sexualliv,
>
> 7.nationell anknytning, eller
>
> 8.brott eller misstanke om brott.
>
> Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet i första stycket.

Mot bakgrund av Datainspektionens tillsynsbeslut om accesskontroll vid granskningen av flera landsting under åren 2013,[44] vilka har genomförts med hänvisning till redan gällande bestämmelser i personuppgiftslagen och vars slutsatser i stort sett redan avgränsat sökningar till det som anges i paragrafen ovan, måste införandet av sådana bestämmelser i flertalet registerförfattningar anses vara överreglering. Motiveringen till denna sorts detaljbestämmelse för hur ett användargränssnitt för en viss applikation på en myndighet ska utvecklas (ty användargränssnitten är den enda plats där denna sorts begränsningar rimligen kan införas) är alltså antingen att kodifiera någonting som väsentligen redan är

---

http://www.datainspektionen.se/press/nyheter/2015/principiella-invandningar-mot-ny-myndighetsdatalag/

[42] *"I sitt yttrande påpekar Datainspektionen att hälso- och sjukvården relativt nyligen fick en ny dataskyddslagstiftning som ökade möjligheterna för spridning av patientuppgifter inom vården, men att Datainspektionens erfarenheter är att den lagen i många avseenden inte följs av vårdgivarna.* Se Datainspektionen, 10 december 2014. http://www.datainspektionen.se/press/nyheter/2014/skarp-kritik-mot-forslag-till-nya-lagar-inom-vard-och-omsorg/

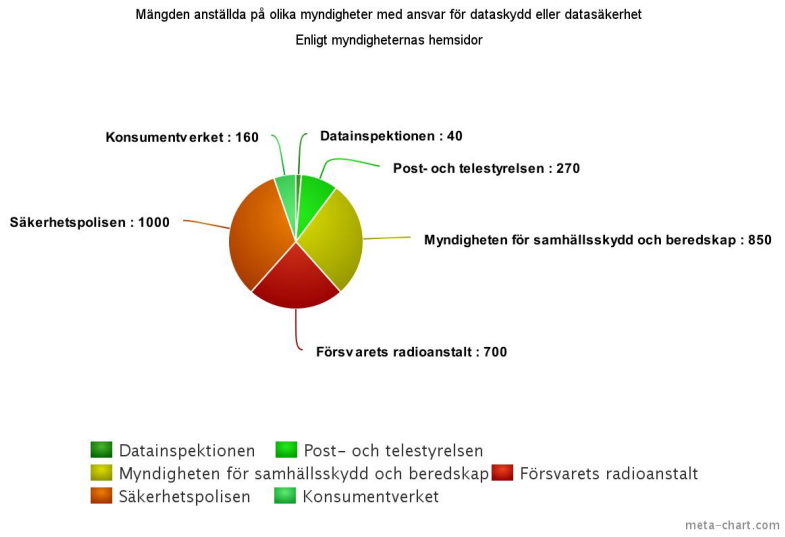
[43] Datainspektionen. Polisen bör anpassa sig till nya polisdatalagen. 28 januari 2014. http://www.datainspektionen.se/press/nyheter/2014/polisen-bor-anpassa-sig-till-nya-polisdatalagen/

[44] Datainspektionen, Datainspektionen granskar samtliga landsting. 16 oktober 2013. Tillgänglig på: http://www.datainspektionen.se/press/nyheter/2013/datainspektionen-granskar-samtliga-landsting/

fallet, eller att begränsa möjligheten för Datainspektionen att utveckla vidare praxis på området. Vidare skapar detaljregleringen en brist på flexibilitet för myndigheterna när de utvecklar sin IT-verksamhet, och minskar utrymmet för innovativa - och kanske mer dataskyddande - åtgärder i framtiden.

En gemensam nämnare i alla registerförfattningar som rör myndigheters verksamhet är föreställningen att individen inte själv ska vara delaktig i uppföljningen av lagstiftningen. Denna föreställning finns redan på utredningsnivå, och de metoder som kan användas för att analysera denna omständighet (till exempel säkerhetsekonomiska modeller) är tillräckligt specialiserade för att man kan anta att de först och främst behöver lyftas med sakkunniga på departement. Lagstiftaren har helt enkelt tillgång till ett torftigt kunskapsunderlag, vilket gör att lagstiftaren även när den försöker ge ett extra starkt skydd för integriteten inte lyckas med detta.

Otillräckliga resurser och tid för dataskydd



Ett enkelt sätt att se varför tillsynen är spretig och medborgarnas skydd är lågt, trots två- eller tresiffriga antal registerförfattningar, många detaljbestämmelser och tre myndigheter med medborgarens bästa för ögonen är att de myndigheter som ska skydda privatpersoner helt enkelt inte har tillräckliga personalresurser. Cirkeldiagrammet framtaget med hjälp av https://www.meta-chart.com

Den 1 oktober 2015 och den 5 oktober 2015 tillkännagav EU-domstolen sina domslut i Weltimmo- och Schrems-målen. Det första rättsfallet har inte rönt särskilt stor medial uppmärksamhet, då det rörde en Slovakien-baserad egendomsagentur som riktade sig mot ungerska privatpersoner.[45] Det andra rättsfallet har fått större uppmärksamhet eftersom det rörde hävande av det så kallade *Safe Harbor*-beslutet som EU-kommissionen fattade om amerikansk lagstiftnings dataskyddande kvaliteter år 2000.[46] Domsluten innebär att nationella datainspektioner i medlemsländerna har ett ansvar att utreda dataskyddsfrågor om dataskyddsfrågan uppstått på en tjänst som riktar sig till invånare i ett visst medlemsland, och att nationella datainspektioner inte kan

Curia C-230/14.

Curia C-364/14.

C-230/14, paragraf 24-26.

[45] Curia (EU-domstolen) C-230/14. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. http://curia.europa.eu/juris/documents.jsf?num=C-230/14

[46] Curia (EU-domstolen) C-364/14. Maximillian Schrems v Data Protection Commissioner. http://curia.europa.eu/juris/liste.jsf?num=C-362/14

hänvisa till utomstående faktorer för att undvika detta ansvar (till exempel ett beslut från EU-kommissionen). Trots att EU-domstolens domar är tydliga, hade Datainspektionen i december 2015 fortfarande inte bestämt sig för om de var kompetenta att utreda dataskyddet på Facebooks servrar i Luleå, enligt uppgift till tidningen UNT.[47]

C-364/14, paragraf 52-54.

I EU-domstolens avgörande i fallet C-201/14, Smaranda Bara m. fl. mot Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF).[48] har domstolen uttalat att

> ”lag /.../ [inte] kan, i den mening som avses i artikel 10 i direktiv 95/46, anses utgöra en information som de registrerade berörda redan känner till och som gör att den registeransvarige befrias från sin skyldighet att informera de personer från vilka inkomstuppgifter har samlats in om vem som är mottagare av uppgifterna.

C-201/14, p. 38.

EU-domstolens beslut gäller utlämnande av personuppgifter från den rumänska skattemyndigheten (ANAF) till den rumänska myndigheten för sjukförsäkringar (CNAS). Utlämningen genomfördes i syfte att bedöma om de berörda privatpersonerna hade rätt till sjukförsäkring. EU-domstolen har funnit att utlämningen inte föregicks av tillräcklig information till privatpersonerna, och att utlämningen därför står i strid mot artikel 10, 11 och 13 (direktiv 95/46/EG).

Dataskydd.net anmälde därför SPAR-registret och tillhörande lagstiftning[49], föreskrifter[50] och personuppgiftsavtal[51] till Datainspektionen som oförenligt med EU:s direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.[52] Att SPAR-registret finns reglerat i lag (1998:527) om det statliga personadressregistret är alltså inte tillräckligt för att utlämningen av personuppgifter till EVRY AB och fler än 1100 andra företag och parter[53] ska anses korrekt. I en separat anmälan, som stödde sig på danska Datatilsynets utredning av stora IT-angrepp på danska myndigheter 2013 och som publicerades i juni 2015[54], menade Dataskydd.net också att SPAR-registret stred mot 31 § personuppgiftslagen om tillräckliga säkerhetsåtgärder.

C-201/14, p. 34.

Datainspektionen fann inte att de hade resurser att utreda detta, och svarade att de väljer ”tillsynsobjekt utifrån ett strategiskt perspektiv. Vi är en liten myndighet som försöker hinna med mycket och vi tar därför tacksamt emot tips, men när vi väljer tillsynsobjekt gör vi det utifrån en helhets analys för att vara så effektiva som möjligt.” Vidare menar Datainspektionen att deras arbete med att upprätthålla nuvarande lagstiftning påverkas negativt ”av att vi även behöver börja arbeta med den nya EU-förordningen.”

[47] UNT, Juriststudent fällde Safe Harbour. 1 december 2015. http://www.unt.se/start/juriststudent-fallde-safe-harbour-3997068.aspx

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

[49] Lag (1998:527) om det statliga personadressregistret

[50] Förordning (1998:1234) om det statliga personadressregistret; Förordning (2007:780) med instruktion för Skatteverket; Skatteverkets föreskrifter om utlämnande av uppgifter ur SPAR (SKVFS 2011:06).

[51] Driftsavtal med företaget EVRY AB sedan 2013.

[52] Se http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:sv:HTML

[53] Se Skatteverkets årsredovisning 2013, s. 68. Tillgänglig på: https://www.skatteverket.se/download/18.15532c7b1442f256bae5a37/1394114494566/16522.pdf

[54] Datatilsynet (Danmark). 31 juli 2015. Journalnummer 2013-632-0050. *Uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for* http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

Det här innebär juridisk osäkerhet för privatpersoner, företag och myndigheter. Det finns ingen som har tid och kapacitet att tolka och tillse gällande rätt. Effektiv tillsyn och snabb rättsskipning ses i alla andra sammanhang än dataskydd som avgörande för rättssäkerheten.[55]

Vi kan förvänta oss att EU-domstolen kommer få en viktigare roll i praxisutvecklingen framöver, då den nya europeiska dataskyddslagstiftningen stärker de ekonomiska sanktionerna för brott mot personuppgiftslagstiftningen ett rejält snäpp. Detta kommer öka behovet av en tillräckligt finansierad Datainspektion, som i tid och med snabbhet kan skapa juridisk säkerhet även i Sverige. I dagsläget verkar det uppenbart att myndigheten inte är rustad för att hänga med, varken tekniskt eller juridiskt.

Negativa ekonomiska incitament för dataskydd

För teknikleverantörerna uppstår det problem eftersom olika lagar säger olika saker. Detta gäller dels över nationsgränser (som de pågående diskussionerna om transatlantiskt dataskydd) men också inom nationer. För ett företag i implementatörsbranschen, utrustningsbranschen eller mjukvarubranschen gäller det att göra en avvägning kring vilken sorts teknisk utveckling som mest sannolikt kommer att ge dem framtida intäkter och så få juridiska bekymmer som möjligt. Detta visar sig sällan vara dataskyddsvänliga lösningar (även om detta kan tänkas förändras med EU:s nya dataskyddslagstiftning, och definitivt har förändrats med så kallad ”*breach notification*”-lagstiftning i USA).

Särskilt om brottsbekämpande myndigheter

Regelverken kring informationstillgång för brottsbekämpande myndigheter är i stort sett de enda integritetsregler som på ett konsekvent sätt upprätthålls. Även om FN:s högsta kommissarie för mänskliga rättigheter, Europarådets kommissionär för mänskliga rättigheter, Europarådets parlamentariska utskott, Europadomstolen i ett flertal rättsfall och EU-domstolen i ett rättsfall uttalar sig emot särskilt massinsamling av personuppgifter,[56] följer inte Sverige deras rekommendationer och bortser ifrån andemeningen i besluten genom att hänvisa till ”sammantagenhet”[57] eller att Sverige skulle ha ett ”särskilt” tillsynsväsende.[58] Det kan så klart vara en intellektuellt tillfredsställande övning att fundera på

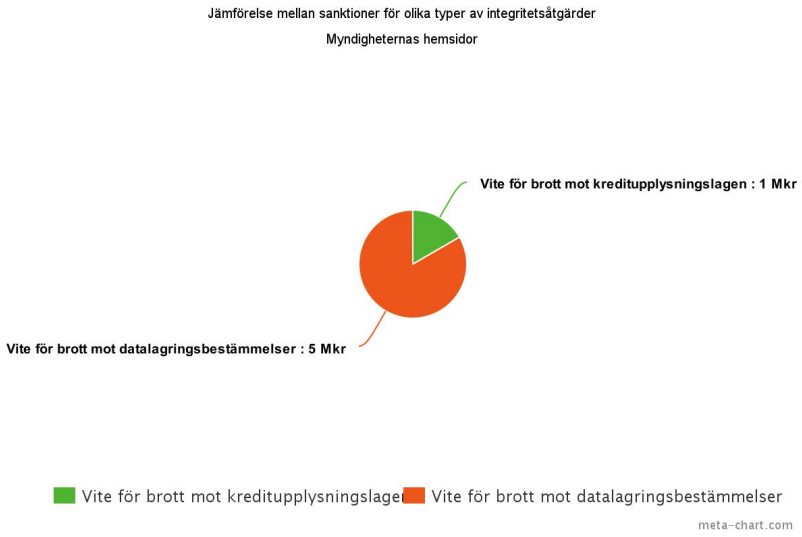
[55] Riksrevisionens rapport RiR 2010:18. Tillgänglig på: http://www.riksrevisionen.se/PageFiles/2086/Anpassad10_18Informationsutbytemellanmyndighetermedansvarförtrygghetssystem.pdf; men se även hänvisningar i SOU 2015:73 till hur bättre informationstutbyten leder till högre rättssäkerhet.

[56] The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights hittas i OHCHR:s dokumentdatabas, tillgänglig på: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=23880; Europarådets människorättskommissionär, CommDH/IssuePaper(2014)1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights*. Se https://wcd.coe.int/ViewDoc.jsp?id=2268589&Site=COE; Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights. Report: Mass surveillance. 26 januari 2015. Rapporteur: Mr Pieter Omtzigt, Netherlands, Group of the European People’s Party; Europeiska domstolen för mänskliga rättigheter i målen *Zakharov v. Russia* (Application no. 47143/06) och *Szabó and Vissy v. Hungary* (Application no. 37138/14); Europeiska unionens domstols dom i de förenade målen C-293/12 och C-594/12.

[57] SOU 2015:31 Datalagring och integritet.

[58] Twitter-diskussion mellan Amelia Andersdotter, en doktorand i IT-rätt vid Stockholms universitet och en professor i juridik vid Uppsala universitet angående Europadomstolens avgöranden i *Zakharov v. Russia* (Application no. 47143/06) och *Szabó and Vissy v. Hungary* (Application no. 37138/14), samt samtal mellan Amelia Andersdotter och en myndighetschef kring samma domslut.

om Säkerhets- och integritetsnämnden är tillräckligt ”särskild” för att i och för sig klara sig igenom Europadomstolens krav på tillsynsmekanism, men det kan inte vara principiellt tillfredsställande att diskussionerna om Sveriges efterlevande av de mänskliga rättigheterna handlar om tolkningsmöjligheterna för ordet ”särskild”.



Dataskydd.net har inte hittat några tillfällen då viten delats ut till följd av brott mot personuppgiftslagen de senaste fem åren. Via Datainspektionens hemsida har ett (1) fall återfunnits då ett kreditupplysningsföretag förelades vidta informationsåtgärder. Detta återges ovan i grönt. Post- och telestyrelsen (PTS) delar regelbundet ut viten till företag som inte följer lagen. Det i diagrammet avbildade vitet är föreläggandet mot Bahnhof att följa reglerna om datalagring i lagen om elektronisk kommunikation.[a] Detta avbildas i rött. Cirkeldiagrammet framtaget med hjälp av https://www.meta-chart.com

[a] PTS, PTS förelägger Bahnhof att lagra uppgifter för brottsbekämpande ändamål. 27 oktober 2014. https://www.pts.se/sv/Nyheter/Telefoni/2014/PTS-forelagger-Bahnhof-att-lagra-uppgifter-for-brottsbekampande-andamal/

Nedan följer fyra exempel på tillfällen då företag bestraffas för att skydda individers integritet, eller belönas för att de inte gör det:

BAHNHOF Internetleverantören Bahnhof försöker minimera mängden uppgifter som lämnas ut till polismyndigheten om deras kunder med hänvisning till EU-domstolens begränsningar för utlämning av datalagrad data till ”särskilt allvarlig brottslighet”. Detta leder till konflikter med både polismyndigheten och Post- och telestyrelsen.

MICROSOFT För att uppfylla EU:s dataskyddsregler, menar Microsoft att amerikanska myndigheter inte kan begära personuppgifter utlämnade som finns på servrar som är fysiskt belägna utanför USA. Amerikanska myndigheter håller inte med utan menar att det är placeringen av Microsofts huvudkontor som är avgörande. Rättskonflikten pågår.

APPLE Som en reaktion på Snowden-avslöjanden införde Apple en ny funktionalitet i sina telefoner som ger användaren ensam makten att bestämma vem som kan komma åt material som sparats på dennes telefon. Just nu pågår en rättskonflikt om huruvida FBI kan tvinga Apple att genomföra en ”uppdatering” av sina telefoner som återställer den gamla funktionaliteten att Apple kan låsa upp telefonen bakvägen och utan användarens medverkan.

MAINTRAC I den statliga offentliga utredningen om lagring av trafikuppgifter (SOU 2007:76) för utredaren upp möjligheten att en tjänstesektor kan utvecklas som hjälper små internetleverantörer som inte själva klarar av kostnaderna att datalagra. Det Linköpingsbaserade företaget Maintrac är ett exempel på en sådan tjänst, som också bidragit till teknisk standardisering av metoder för förenklad polisiär tillgång till trafikuppgifter i realtid.

IT-organisationen på myndigheter

Danska Datatilsynet fann följande vid en granskning av stora dataintrång på danska myndigheter 2013:[59]

> [a]t hackerangrebet førte til, at bl.a. oplysninger i Schengen-informationssystemet er blevet overført til hackerens computer i Cambodia, må overvejende tilskrives /.../ for omfattende deling af IT-systemmæssige ressourcer som LPAR, operativsystem, diske og RACF mellem de forskellige dataansvarlige[.]
>
> Datatilsynet, 2013-632-0050

Av den danska tillsynsrapporten kan man dra slutsatsen att de krav som ställs på offentliga IT-system inte lånar sig till dataskyddande, eller ens datasäkra, lösningar. Problemet med kravställningar vid IT-upphandlingar är ett återkommande tema i statliga utredningar om informationssäkerhet sedan 40 år.[60] Idag förutsätter dock lagstiftaren att myndigheterna ska samverka med varandra på ett sådant sätt att det knappast är tänkbart att IT-systemen skulle kunna bli mer dataskyddande eller datasäkra. Riksrevisionen efterfrågar i själva verket mer dataöverföringar mellan myndigheter i syfte att uppnå effektivisering.[61]

Dataskydd.net vill lyfta forskning från Linköpings universitet som föranleder frågeställningen om det inte är så att myndigheter använder sig av informationsteknologi för att kunna fatta *fler* beslut *snabbare* och av *fler olika* karaktär.[62] Om en förbättrad möjlighet att fatta beslut leder till att man inför en massa nya beslut som måste fattas, är det inte säkert att informationsteknologin någonsin kommer ha potential att innebära reella effektiviseringar. Se också Gabriella Janssons doktorsavhandling om elektronisk förvaltning i Botkyrka kommun, med tillhörande resonemang om e-förvaltning som ett sätt att skjuta över ansvar för förvaltningen av medborgarna på medborgarna själva.[63] En sådan ansvarsförskjutning kan också innebära att individen också får ett - felaktigt och på grund av brist på transparens svårbevakat - ansvar för sitt eget integritetsskydd vid kontakter med förvaltningen.

Frågorna kan tyckas enbart perifert kopplade till dataskydd, men utifrån Datatilsynets utredning är det uppenbart att de hör ihop. Möjligheten för individer

[59] Datatilsynet (Danmark). 31 juli 2015. Journalnummer 2013-632-0050. *Uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for* http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

[60] För en någorlunda komplett sammanställning, se https://dataskydd.net/svenska-utredningar-om-dataskydd med tillhörande länkar.

[61] Informationsutbyte mellan myndigheter med ansvar för trygghetssystem (RiR 2010:18). Tillgänglig på http://www.riksrevisionen.se/PageFiles/2086/Anpassad%2010_18%20Informationsutbyte%20mellan%20myndigheter%20med%20ansvar%20f%C3%B6r%20trygghetssystem.pdf

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

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

att utöva sina rättigheter är tätt sammankopplad med förmågan hos beslutsfattare och tjänstemän att utforma digitala miljöer på ett sådant sätt att transparens, begriplighet, förutsägbarhet och säkerhet gentemot individer är möjlig. Dataskyddslagstiftningens principer för ändamålsbegränsning, dataminimering och samtycke är här ett stöd, som hjälper med den grundläggande design-tanken i ett IT-system. Denna möjlighet underutnyttjas av både lagstiftare och myndigheter, som istället verkar förutsätta att dataskyddsprinciper är någonting man måste skapa undantag ifrån då man utvecklar myndigheternas verksamhet.[64]

Kravställning utan dataskydd

Konsumenter som försöker skydda sitt privatliv, till exempel genom att använda insticksprogram i sin webbläsare, stöter på varningar från både myndigheter och företag. Ett exempel är de små lådorna som inhämtar samtycke för att placera kakor på webbplatsbesökarens dator. Formuleringar som ”*tryck okej så hjälper du oss att göra en bättre webb*” ger intrycket av att konsumenten har en skyldighet att hjälpa webbutvecklaren känna sig tryggare i sin yrkesroll, och att ett misslyckande att underlätta webbutvecklarens arbete innebär en försämring av webben. Att vilja skydda sina rättigheter bör emellertid inte framställas som någonting subversivt eller dåligt.

Vid kontakter med privata företag, till exempel dagstidningar, kan man tänka sig att tidningens webbutvecklare vill förvänta sig en motprestation från läsaren motsvarande prenumerationsavgifter och att en skyldighet för besökaren att godkänna tidningens villkor för att få vara på webbplatsen är befogad.

Meddelanden om att beteendekartläggning är oumbärlig för att internet ska kunna förbättras och webben vara bra finns dock även på svenska regeringens hemsida samt flertalet kommuner och landstings hemsidor.[65] Avsaknaden på politiskt ledarskap kring vad som är en medborgerlig förpliktelse och vad som är en medborgerlig rätt leder till slentrianmässig kartläggning av enskilda som inte bara är obefogad utan också missledande och i värsta fall redan olaglig. Eftersom den offentliga verksamheten inte tänker på att detaljerad statistik över besökarna måste framställas på ett sätt som innebär en kränkning av individens rätt till privatliv, kan man tänka sig att verksamheten av nyfikenhet specificerar att de vill ha sådan statistik över webbplatsbesökarna. Detta är ytterligare ett negativt incitament för dataskydd eftersom en sådan webbyrå som har en dataskyddande inriktning på verksamheten riskerar att inte få kontrakt.

Genom Dataskydd.net:s kontakter med bland annat Enköpings kommun under 2015[66] har det också framkommit att det är svårt att få råd från statliga myndigheter om vad som egentligen gäller för spårning och beteendekartläggning. Stora kampanjer mot tredjepartsspårning från ett flertal större amerikanska aktörer har höjt medvetenheten bland webbutvecklare och konsumenter kring webbanalysverktyg, men Datainspektionen menar att det beror på ifall kartlägg-

[64] Se Dataskydd.net:s inlaga till spelutredningen av den 5 februari 2016: https://dataskydd.net/sites/default/files/dataskydd_spelutredningen_inlaga_20160128.pdf, eller motsvarande Föreningen för digitala fri- och rättigheters inlaga till spelutredningen av den 10 februari 2016: https://www.dfri.se/wp-content/uploads/2016/02/dfri-illegal_spelverksamhet_m_dataskydd.pdf

[65] Se Dataskydd.net:s forskning kring spårningsverktyg och övervakningsmöjligheter vid besök på kommunala hemsidor, presenterade till exempel på FSCONS 2015: https://dataskydd.net/fscons-2015

[66] Se http://blogg.enkoping.se/webbutveckling/tag/dataskydd-net/

ningen faller under personuppgiftslagstiftningen. *Best practises* saknas i industrin för webbutveckling: lokal webbanalys, TSL- eller SSL-kryptering för alla anslutningar till hemsidan, borttagande av referrer-headers, användning av *security headers* samt länkar till sociala medier som inte ”rapporterar” vad användaren gör till mediaplattformen är inte tekniskt svåra åtgärder. Till skillnad från tillgänglighetskrav finns inga nationella riktlinjer för kommuner att förhålla sig till. En leverantör av *text-to-voice*-tjänster (ett webbutvecklingskrav enligt centralt framtagna mallar för hemsideutveckling) som Dataskydd.net granskade närmare hävdar i sitt dataskyddsavtal att de, med avseende på insamling av personuppgifter, inte kunde ta ansvar för om tjänsterna de levererade spårade användaren mer än vad de var medvetna om. Här finns två problem: ingen har ställt kravet på leverantören att veta vad som gäller för tjänsterna de levererar, och företaget tycker uppenbarligen självt att det är lugnt att leverera sådant man inte vill ta ansvar för. Arbetet med att granska *text-to-voice*-tjänster kommer att fortsätta under våren, och Dataskydd.net har som målsättning att initiera direkt kontakt med de fyra vanligaste tjänsterna (Insipio, Readspeaker, Browsealoud och Funka).

Underutnyttjande av möjligheterna till teknisk standardisering för dataskydd

Idag saknas teknisk standardisering till integritetens fördel, trots att integritet bedömts som så viktigt att det är en del av samtliga existerande konventioner om mänskliga rättigheter. Även när det finns processer för tillsynsmyndigheter att engagera sig i standardiseringsprocesser, gör de det inte. Även när det finns tekniska standarder, används de inte.

RFID: det enda framgångsexemplet

Det finns bara 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).[67]

E-leg och DNT: Standardiseringsprocesser 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)[68] eller medlemsländernas satsningar (t ex svensk e-legitimation) inkorporerat integritetsfrämjande resultat. I Sverige har Karlstads universitet

http://FIDIS.net

https://abc4trust.eu

[67] http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32009H0387&from=EN

[68] Kommissionens ursprungliga förslag till e-legitimationsförordning försökte istället förbjuda anonym autenticering. ”*[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.*” Se 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

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.

http://prisec.kau.se/

I andra standardiseringsprocesser, till exempel Do Not Track-gruppen[69] 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 hemsideförvaltarna, 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,[70] och EU-kommissionens engagemang var begränsat till ett antal offentliga yttranden från den dåvarande kommissionären.

Randomiserade identifierare: dataskyddsstandardisering 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.[71] Nederländska datainspektionen kom fram till en liknande slutsats i december 2015.[72] Samtidigt har vissa större teknikleverantörer, däribland Apple, experimenterat med ”randomiserade initiala identifierare” (i detta fall MAC-adresser).[73] 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.[74] Som ett ”väsentligt krav” på radioutrustning omnämns 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.

Direktiv 2014/53/EG, artikel 3(3)(e).

---

69 https://www.w3.org/TR/tracking-dnt/

70 https://www.w3.org/2000/09/dbwg/details?group=49311&public=1

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

72 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

73 Se t ex http://blog.mojonetworks.com/ios8-mac-randomgate/

74 Se http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32014L0053

Smarta elmätare: standardisering som struntar i dataskydd

Ei R2015:09

I en utredning om funktionskrav på smarta elmätare[75] framställd av Energimarknadsinspektionen förra året lämnade Energimarknadsinspektionen all diskussion om dataskydd och IT-säkerhet därhän med hänvisning till att tillverkarna av smarta elmätare upplever att deras produkter redan är säkra. Smarta elmätare är kända för att vara häftade med ett stort antal dataskydds- och säkerhetsproblem: 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.[76] 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, istället 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.

Många regler om samma sak

En egenhet i dataskydds- och datasäkerhetslagstiftningen är att samma regler kan återfinnas på flera olika ställen i lagstiftningen utan att för den delen ha önskad effekt.

Fyra gånger incidentrapporter

En incidentrapport är en rapport till antingen en myndighet eller en berörd privatperson om att någonting i ett IT-system har gått fel. Sverige kommer att ha fyra separata förpliktelser att incidentrapportera från och med våren 2018:

- EU:s direktiv 2002/58/EG om skydd av personuppgifter i elektroniska kommunikationsnät (”ePrivacy-direktivet”) ålägger telekomoperatörer att avlägga incidentrapporter vid säkerhetsproblem i nätet. EU-kommissionens förordning 2013/611 specificerar regelverket för dessa incidentrapporter.[77]
- EU:s direktiv 2015/**/EG om nätverkssäkerhet[78] ålägger en ännu okänd mängd marknadsaktörer att avlägga incidentrapporter till någon koordinerande myndighet i medlemsländerna.
- EU:s allmänna dataskyddsförordning ålägger personuppgiftsansvariga och personuppgiftsbiträden att rapportera incidenter till tillsynsmyndigheten

[75] Se http://www.energimarknadsinspektionen.se/sv/Publikationer/Rapporter-och-PM/rapporter-2015/funktionskrav-pa-framtidens-elmatare-ei-r2015-09/

[76] Broberg, Thomas. Brännlund, Runar. Kazukauskas, Andrius. Persson, Lars. Vesterberg, Matthias, ”En elmarknad i förändring – Är kundernas flexibilitet till salu eller ens verklig?” Umeå universitet, augusti 2014. Rapport beställd av Energimarknadsinspektionen. Tillgänglig på http://ei.se/Documents/Publikationer/rapporter_och_pm/Rapporter%202014/Rapport_en_elmarknad_i_forandring_Umea_universitet.pdf

[77] Se http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1456015407642&uri=CELEX:32013R0611

[78] Se http://www.consilium.europa.eu/en/workarea/downloadAsset.aspx?id=40802207457

(Datainspektionen) och eventuellt också till privatpersoner från och med ikraftträdandet av förordningen.[79]

- MSB kommer från och med april 2016 ålägga statliga myndigheter att formulera incidentrapporter då IT-incidenter har inträffat.[80]

Dataskydd.net har framhållit i ett antal remissyttranden under 2015 att rapportering direkt till privatpersoner är det mest önskvärda.[81] Vi baserar denna bedömning på erfarenheterna från amerikanska delstater så som Kalifornien.[82] Eftersom incidentrapporteringar direkt till slutkonsument redan funnits i över ett decennium i USA, finns det gott om utredningar om både de ekonomiska effekterna och fördelarna för konsumenter (företrädelsevis möjligheten att ställa företag och myndighet till svars som inte uppfyllt sina säkerhetsförpliktelser gentemot individer). Dataskydd.net rekommenderar Romanosky (2010).[83]

Det finns inga europeiska krav på att ett medlemsland ska gå så långt i sin konsumentupplysningsverksamhet att samtliga incidenter då personuppgifter hamnat på villovägar ska rapporteras till privatpersonen själv. Dataskyddsförordningen kommer närmast, det finns ingenting som hindrar Datainspektionen från att tolka förordningen så att privatpersoner i så hög utsträckning som möjligt ska ges tillräcklig information för att utkräva ansvar från myndigheter och företag vars informationssäkerhetsarbete brustit.

Två gånger spårning

Insamling av besöksinformation i kartläggningssyfte regleras i både personuppgiftslagen och i lagen om elektronisk kommunikation. Dessa lagar har dock olika tillsynsmyndigheter. Enligt information som Dataskydd.net har fått genom kontakter med myndigheterna gäller det att medan Datainspektionen inte känner att de kan utreda kartläggning av individer i digitala miljöer på grund av Post- och telestyrelsens tillsynsansvar, upplever sig Post- och telestyrelsen inte kunna utföra en tillräcklig tillsyn på grund av att de inte har tillgång till de mer principiella bestämmelserna i personuppgiftslagen. Möjligheterna för samverkan mellan myndigheterna förefaller vara begränsade.

Amelia Andersdotter
Ordförande, Dataskydd.net

[79] Se http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/sv/pdf

[80] Se https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nytt-informationssakerhet/Obligatorisk-it-incidentrapportering-infors-1-april-for-statliga-myndigheter/

[81] Se yttranden över SOU 2015:23, SOU 2015:39, SOU 2015:73 på https://dataskydd.net/vara-remissvar

[82] Se https://oag.ca.gov/ecrime/databreach/reporting

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