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 2016-03-18

Inlaga till utredningen om tillsynen över den personliga integriteten Ju 2015:02

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 tekniskt möjliga påverkar individers möjlighet till

självbestämmande i digitala miljöer. För närvarande är verksamheten avgränsad till hemsidor.

Dataskydd.net har läst utredningens uppdrag så att utredningens syfte är att stärka skyddet för den personliga integriteten. Detta övergripande syfte anser Dataskydd.net bör vara vägledande för utredningens övriga arbete, och utredningen kan, om den ska lägga förslag för detta syfte, inte begränsa sin analys av tillsynen till de myndigheter som exemplifieras i uppdragsbeskrivningen. Vi har noterat att tidigare utredningar påpekat brister vid utarbetande av integritetsstärkande lagstiftning. En orsak till dessa brister anser vi vara att utredningarna inte anammar ett syftesinriktat perspektiv. Dataskydd angår näringspolitik, rättspolitik och teknisk standardisering. Tillsyn och rekommendationer på ett av dessa områden påverkar förutsättningarna för tillsyn och rekommendationer på andra.

SOU 2007:22, s. 445.

Datasäkerhet vs dataskydd

Dataskydd.net har märkt att svenska utredningar saknar en bra distinktion mellan datasäkerhet och dataskydd. Trots att distinktionen saknas används begreppet ”integritetsstärkande” ofta synonymt med begreppet ”datasäkerhetsstärkande”. Ibland kan ”integritetsstärkande” innebära en integritetskränkning med extra administrativa bördor för det allmänna. Utredningen om datalagring påtalar till exempel ökad granskning av säkerhetsrutiner hos teleoperatörerna som en ”integritetsstärkande” åtgärd, och att hårdare kontroller av teleoperatörernas datorsystem innebär en ökad rättssäkerhet. Det verkar missledande: integriteten stärks inte av datalagring, som i och av sig själv konstaterats negativ för utövandet av de mänskliga rättigheterna av bland andra FN, Europarådet och Europeiska unionens domstol. Det man stärker är datasäkerheten.

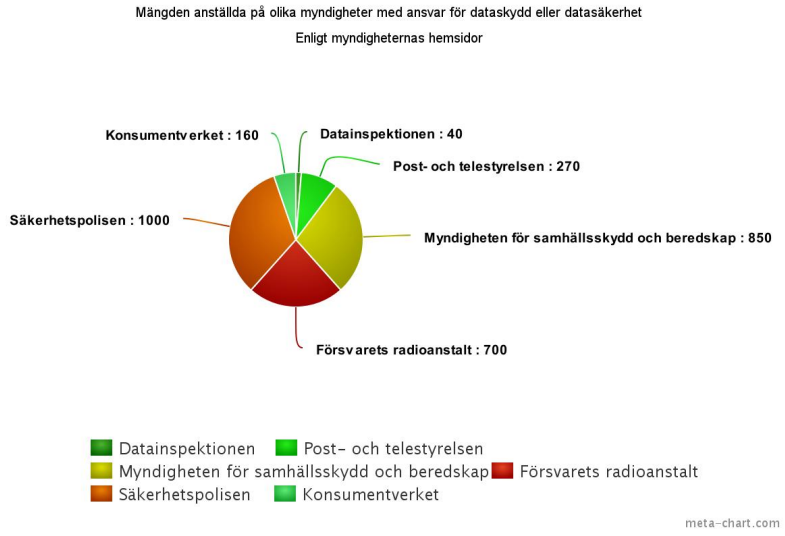
Därför föreslår Dataskydd.net följande distinktion: datasäkerhet är när ett system fungerar som det är tänkt. Det är möjligt att ha ett säkert system som kränker individens rätt till privatliv och dataskydd. Dataskydd är att ett system fungerar på ett sådant sätt att individens rättigheter respekteras. Ett dataskyddande system måste vara säkert, men ett säkert system måste inte vara dataskyddande. En bra uppdelning mellan datasäkerhet och dataskydd tillåter utredaren och lagstiftaren att förstå när statens intresse av att individers rättigheter skyddas och statens intresse av att skydda sig själv hamnar i konflikt med varandra. Det minskar också risken att lagstiftaren drar den felaktiga slutsatsen att ett stärkt skydd av staten per automatik innebär ett starkare skydd för individer.

Tillsyn för säkerhet och dataskydd

I utredningsuppdraget nämns bara ett fåtal av de myndigheter som idag ansvarar för dataskydd och datasäkerhet. För att förstå bristerna i dagens tillsyn av integritetsskyddet behöver man jämföra de konsument- och individinriktade tillsynsverksamheterna med de myndigheter och verksamheter som bevakar andra intressen än individens. Som kommer att framgå finns det gott om tillfällen då intressekonflikter mellan olika aktörer (individer, myndigheter, företag) och olika inriktad tillsyn för dessa verksamheter har negativa konsekvenser för individers möjligheter att utöva sina rättigheter.

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. I 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 2015 påtalas 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 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 till privatpersoner: säker identitetsinformation och anti-virusprogram hjälper privatpersoner att agera på ett sätt som är så effektivt för banker och myndigheter som möjligt.



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

Då Myndigheten för samhällsskydd och beredskap samt Försvarets radioanstalt är ansvariga för datasäkerhetsåtgärder på myndigheter, följer att myndigheternas IT-åtgärder präglas av ett fokus på institutionell datasäkerhet, snarare än på individuellt dataskydd.

[1] Myndigheten för samhällsskydd och beredskap [https://www.dinsakerhet.se/]

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

Exempel på när allmänhetens och det allmännas intressen kan gå isär

Ovan nämnde vi att Myndigheten för samhällsskydd och beredskap valt att utforma sina säkerhetstips till privatpersoner 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 skriptblockerare) som installerats i deras webbläsare, gav Myndigheten för samhällsskydd och beredskap ett nekande svar (för mer om detta, se nedan).

Detta är inte det enda exemplet som finns på hur statlig säkerhet och individuell säkerhet inte är samma sak. Dataskydd.net väljer först att exemplifiera ett antal situationer där myndigheters och individers intressen av dataskydd inte är överensstämmande, och som inte rör brottsbekämpande verksamhet:

Datadelning som gör det svårare för privatpersoner att utöva sina individuella rättigheter verkar motiveras med att det kan utgöra en kontrollåtgärd mot myndigheternas tjänstemän. Riksrevisionen skriver att ”bristande informationsutbyt[e] leder /.../ till ökad risk för felaktiga utbetalningar, eftersom den manuella kontrollen är så tidskrävande för handläggarna att de ibland väljer att avstå från att göra den,” som om att effektivitetsproblemet på myndigheterna handlar om tjänstemän med bristande moral. Av Riksrevisionens rapport framgår inte om den ökade risken går att kvantifiera. RiR 2010:18, s. 63

De studier om effektivitet vid distansbetjäning från myndigheterna mot medborgarna verkar visa att organisatoriska brister bortom privatpersonens kontroll gör systemen ineffektiva, snarare än att det skulle finnas en brist på datadelning, IT-system eller medborgardisciplin.[3] VAB-reformen genomfördes 2012-2013 för att underlätta för föräldrar och spara administrationskostnader hos Försäkringskassan – den har lett till något fler felaktiga utbetalningar,[4] men nyttan av reformen kan sammantaget ändå ha uppnått sitt mål. Chefer från Försäkringskassan har istället för att utvärdera eventuella effektiviseringar vänt sig till media för att efterfråga fler kontrollåtgärder mot privatpersoner.

Statskontoret har indikerat att behovet av arbetskraft och arbetstid på myndigheterna går uppåt snarare än nedåt [5]. Om behovet av årsarbetskrafter går upp trots två årtiondens flitiga investeringar i e-förvaltning och bättre möjligheter att överföra och dela personuppgifter mellan olika verksamheter, finns anledning att inte anta varken korrelation eller kausalitet mellan mer datadelning och effektivisering.

Angående brottsbekämpande myndigheter har FN:s högsta kommissarie för mänskliga rättigheter, Europarådets kommissionär för mänskliga rättigheter, Europarådets parlamentariska utskott, Europadomstolen i ett flertal avgöranden och EU-domstolen i ett avgörande uttalat sig emot särskilt massinsamling av personuppgifter.[6]

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

[4] Martinsson, A (2015, november, 3) ”Fler åker fast för vab-fusk”, Göteborgsposten, [https://www.gp.se/nyheter/sverige/1.2884301-fler-aker-fast-for-vab-fusk]

[5] Statskontoret, 2015. ”Förändringar i svensk statsförvaltning och framtida utmaningar”, s 59 [http://www.statskontoret.se/publikationer/2015/forandringar-i-svensk-statsforvaltning-och-framtida-utmaningar/]

[6] United Nations High Commissioner for Human Rights, ”The right to privacy in the digital

Av särskilt intresse är FN:s högsta kommissarie för de mänskliga rättigheternas rapport av den 30 juni 2014,[7] som i punkt 42 observerar att de brottsbekämpande myndigheternas intressen ges företräde över individers rätt att utöva sina mänskliga rättigheter vid standardiseringen av teknisk utrustning. Detta gäller både på det övergripande planet, i telekommunikationsinfrastrukturen (vilket var vad den högsta kommissarien avsåg i sitt uttalande) och på mikronivå, vid standardiseringen av elektronik för slutkonsumenter (detta har uppmärksammats av den högsta kommissarien senare[8]).

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 kan datalagra på ett kostnadseffektivt sätt. 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.

Brist på sanktioner för dåligt beteende

Enligt vad Dataskydd.net erfar är de administrativa sanktionerna för att inte tillfredsställa polisens krav på intrång i integriteten i Sverige runt fem gånger

age”, [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. [https://wcd.coe.int/ViewDoc.jsp?id=2268589&Site=COE]; Omtzigt, P. 26 januari 2015. Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights. ”Report: Mass surveillance”.; 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.

[7] United Nations High Commissioner for Human Rights, ”The right to privacy in the digital age”, [http://ap.ohchr.org/documents/alldocs.aspx?doc_id=23880]

[8] OCHCR. ”Apple-FBI case could have serious global ramifications for human rights: Zeid”. 4 mars 2016. [http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E]

högre än de ekonomiska sanktionerna för att inte tillfredsställa lagtiftarens krav på skydd av den personliga integriteten. Vi har tagit fram de uppgifterna genom att jämföra viten utdelade av Post- och telestyrelsen för brott mot lagen om elektronisk kommunikations krav på datalagring[9] och tillsynsärenden vid Datainspektionen (som uppger att de delat ut två viten om en miljon kronor vardera för kränkningar av lagen om kreditupplysningar). Centrum för rättvisas stämning mot Västerbottens landsting resulterade i ett skadestånd för den enskilde på 10000 kronor.[10]

Om en privatperson försöker utöva sin egen rätt till dataskydd är alltså skyddet fem hundra gånger svagare än om staten försöker skydda sina intressen. Även om man ska vara försiktig med att låta så kallad *rational choice*-teori styra ens världsbild, kan man inte heller avfärda intrycket av att incitamenten att motarbeta individers möjligheter utöva sina rättigheter är betydligt starkare än incitamenten att stärka dessa möjligheter.

Effektivitet, rättssäkerhet och dataskydd

Det finns många exempel på när statliga utredningar har definierat rättssäkerhet och effektivitet som antagonistiska mot dataskydd och skyddet för den personliga integriteten. I utredningen om en ny myndighetsdatalag ställs dataskydd i motsatsförhållande till effektivitet vid minst sju tillfällen. Riksrevisionen har också påtalat hur ett svagare integritetsskydd stärker effektiviteten i myndigheterna.[11] E-delegationen positionerar också dataskydd och effektivitet mot varandra. En påstådd konflikt mellan rättssäkerhet och effektivitet å ena sidan, samt dataskydd å andra sidan, återfinns explicit i utredningen om en ny utlänningsdatalag. Det är framför allt individens möjlighet att förstå varför och hur data delas mellan olika aktörer (i ovanstående fall i offentlig sektor) som utredningarna upplever står i strid med myndigheternas målsättning att effektivisera sin verksamhet.

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

RiR 2010:18.

SOU 2014:75, s. 103. SOU 2014:39, s. 16. SOU 2013:22, s. 36. osv.

SOU 2015:73, s. 185–186.

Brist på rättssäkerhet kan antas uppstå om dataskydd och personlig integritet inte tilldelas tillräckliga tillsynsresurser.

I Belgien befanns Facebook hösten 2015 olovligen ha spårat icke-medlemmar när dessa besökte andra hemsidor än Facebook. Simon Davies, en brittisk dataskyddsförespråkare, har i samband med detta påtalat att de hemsidor som hjälpte Facebook spåra icke-medlemmarna uppfyllt de kriterier som belgiska Privacy Commission ställt upp för att insamla samtycke för spårning.[12] Man kan inte utesluta att sådana felaktigheter uppstår även i Sverige: EU-domstolens

[9] 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/]

[10] Centrum för rättvisa. ”Vårdtagare mot Västerbottens läns landsting”. [http://centrumforrattvisa.se/aktuella-fall/vardtagare-mot-vasterbottens-lans-landsting/]

[11] 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-/]

[12] Simon Davies (Privacy Surgeon). ”The Belgian decision about Facebook cookies has huge data protection and press freedom implications”. December 2015. [http://www.privacysurgeon.org/blog/incision/the-belgian-decision-about-facebook-cookies-has-huge-dataprotection-and-press-freedom-implications/]

beslut att kommissionens beslut om dataöverföringar till USA var ogiltiga hösten 2015 är till exempel ett sådant fall där Datainspektionen direkt uppmanats i media, av ledande experter på området, att inte tillse lagstiftningen eller utfärda undantag från tillsyn.[13] Notera att fall då företag blir fällda i domstol trots att de följt Datainspektionens implicita rekommendationer kan bli en kostnad för företagen även om de inte döms att betala höga skadestånd: att befinnas ha stridit mot dataskyddslagstiftningen och individers rättigheter skapar till exempel *good will*-förluster. Risken för *good will*-förluster har studerats vid bland andra Handelshögskolan i Stockholm.[14]

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 medial uppmärksamhet. Det rörde Slovakien-baserad egendomsagentur som riktade sig mot ungerska privatpersoner.[15] Det andra rättsfallet har fått uppmärksamhet och rör hävande av det så kallade *Safe Harbor*-beslutet som EU-kommissionen fattade om amerikansk lagstiftnings dataskyddande kvaliteter år 2000.[16] 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 hänvisa till utomstående faktorer för att undvika detta ansvar (till exempel ett beslut från EU-kommissionen). Datainspektionen hade i december 2015 fortfarande inte koll på vilken lag som gäller för Facebooks servrar i Luleå, enligt uppgift till tidningen UNT.[17]

Curia C-230/14.

Curia C-364/14.

C-230/14, paragraf 24-26.

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).[18] 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.

Dataskydd.net anmälde SPAR-registret och tillhörande lagstiftning[19], föreskrifter[20] och personuppgiftsavtal[21] 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.[22]

[13] IDG, ””Det kommer att bli tumultartat” – ovisst för företagen efter safe harbor-domen”. 6 oktober 2015. [http://www.idg.se/2.1085/1.638827/safe-harbor]

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

[15] 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]

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

[17] Upsala Nya Tidning, ”Juriststudent fällde Safe Harbour”. 1 december 2015. [http://www.unt.se/start/juriststudent-fallde-safe-harbour-3997068.aspx]

[18] 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]

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

[20] 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).

[21] Driftsavtal med företaget EVRY AB sedan 2013.

[22] Europeiska gemenskapernas officiella tidning. ”Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter”. [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:sv:HTML]

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[23] 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[24], menade Dataskydd.net också att SPAR-registret stred mot 31 § personuppgiftslagen om tillräckliga säkerhetsåtgärder.

C-201/14, p. 34.

Datainspektionen hade inte 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.”

Att Datainspektionen inte kan utreda vad det rådande rättsläget är på grund av det framtida rättsläget innebär juridisk osäkerhet för privatpersoner, företag och myndigheter. Nedan följer ytterligare exempel på hur tillsynen fungerar dåligt, med dålig översikt och förutsägbarhet för företag och individer som resultat:

Lagar som inte följs, tillsynsbeslut som lagstiftas runt

När Datainspektionens observationer om särskilt vårdverksamhet[25] och polisverksamhet[26] indikerar att lagstiftning, även när den tar vissa integritetsaspekter i beaktande, inte efterlevs, händer däremot ingenting.

Man kan tänka sig att detta har att göra med svårigheten för individer att få reda på när lagar inte följs, och bristande möjligheter för individer att åsamka den felande parten sanktioner även då detta uppdagas (se ovan).

Dataskydd.net:s arbete med propositioner om registerförfattningar under hösten 2015 indikerar att även då Datainspektionen genomför tillsyn, så arbetar sig utredningar, myndigheter och lagtiftaren runt resultatet av tillsynen. Dataskydd.net granskade samtliga tillsynsbeslut som Datainspektionen fattat med stöd av 30-31 §§ personuppgiftslagen. I dessa framgår sedan 2010 att accesskontroll måste vara utformad på ett sådant sätt att bara de uppgifter som strikt behövs för att någon ska utföra en viss arbetsuppgift ska vara tillgängliga för denna. Som svar på detta har Justitiedepartementet i samtliga propositioner om nya registerförfattningar under hösten 2015 lagt in en bestämmelse om sökbegränsningar. Motiveringen för en detaljreglering för hur ett användargränssnitt

Propositioner:

Prop. 2014/15:143
Prop. 2014/15:148
Prop. 2015:16/28
Prop. 2015/16:65

[23] Skatteverket. ”2013 Årsredovisning”, s 68. [https://www.skatteverket.se/download/18.15532c7b1442f256bae5a37/1394114494566/16522.pdf]

[24] 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/]

[25] Datainspektionen, 10 december 2014. ”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.” [http://www.datainspektionen.se/press/nyheter/2014/skarp-kritik-mot-forslag-till-nya-lagar-inom-vard-och-omsorg/]

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

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 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.

Det tydligaste exemplet på kringgående av Datainspektionens tillsynsbeslut är den lag som tillkom för att skydda och möjliggöra projektet *LifeGene* vid Karolinska institutet. I december 2011 fann Datainspektionen att respekten för individers rättigheter vid projektets utformning inte var tillräcklig.[27] På mindre än ett år utarbetades ett lagförslag om hur man kunde kringgå Datainspektionens tillsynsbeslut.[28]

Det kan inte anses förvånande att tillsynen i Sverige inte är effektiv eller ändamålsenlig när tillsynen, även då den sker, enbart har till resultat att lagar skrivs som undantar den tillsedda verksamheten från integritetsskyddande förpliktelser. Det är så klart ytterst ett politiskt problem, men utredningen gör regeringen och sig själva en otjänst om utredningen inte påtalar detta. För beslutsfattare som ofta måste hantera många olika frågeställningar samtidigt är det inte alltid uppenbart när den politiska inriktningen hamnar i konflikt med sig själv, och utredningsväsendet är det enda verktyg de politiska beslutsfattarna kan förlita sig på för att upptäcka sådana konflikter.

Tillsyn i EU:s dataskyddsförordning

I EU:s nya dataskyddsförordning, som väntas träda i kraft under våren 2018, stärks de administrativa sanktionerna för brott mot dataskyddslagstiftningen. Detta innebär väsentligt högre krav på Datainspektionen att i tid och med effektivitet utföra sitt arbete: om Datainspektionen inte får tillräckliga resurser att göra detta, riskerar företagen att drabbas av höga kostnader.

Särskilt om organisationer som representerar individer

Lagstiftningen innehåller, precis som den svenska diskrimineringslagen, en bestämmelse om att privatpersoner ska ha en rätt att utse en organisation att representera dem i dataskyddsprocesser. Av demokratiskt intresse för EU är 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.[29] Här kan Sverige agera positiv demokratisk förebild genom att

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

[27] Datainspektionen. ”Tillsyn enligt personuppgiftslagen (1998:204)”, PuL. LifeGene. Dnr 766-2011 [https://www.datainspektionen.se/Documents/beslut/2011-12-19-lifegene.pdf]

[28] Karolinska Institutet, ”LifeGene får fortsätta”. [http://ki.se/nyheter/lifegene-far-fortsatta]. Lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa. [http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Lag-2013794-om-vissa-regist_sfs-2013-794/?bet=2013:794]

[29] Ett analogt exempel är ungerska regeringens misslyckade försök att etablera en ny dataskyddsmyndighet, vars direktör enklare kunde avsättas politiskt, 2012. Se omständigheterna kring

frångå de detaljerade krav på organisationer med möjlighet att representera privatpersoner som återges i diskrimineringslagen.

I förordningens skäl 112 presenteras också möjligheten för medlemsländerna att grupper från civilsamhället att driva principiella rättsfall utan att ha en enskild målsägande. Denna möjlighet finns redan i konsumentskyddslagstiftningen i Sverige, och gör det möjligt för till exempel organisationen Sveriges konsumenter att anmäla företag som har oskäliga avtalsvillkor till Konsumentverket.[30]

GDPR, skäl 112.

Det är av grundläggande intresse för det effektiva utövandet av och skyddet för de mänskliga rättigheterna till dataskydd och integritet att individer och organisationer ges möjlighet att agera för skyddet av individer även utan behöva förlita sig på att en viss oförrätt ska hamna i en myndighets tillsynsplanering. Bland annat Centrum för rättvisa har i Sverige demonstrerat att det är både relevant och effektivt att låta rättighetskämpar ”gå före” i utvecklingen.[31]

Integritetsombudsman

Notera att frågan om ombudsmannafunktion också är under prövning av EU-domstolen i målet C-192/15, Rease.[32]

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.[33]

Datainspektionen är en ”nej-sägare”

Datainspektionens nuvarande verktygslåda har nackdelen att Datainspektionen bara *ex post* kan dyka upp och berätta för det allmännas och näringslivets aktörer att de har haft fel. Detta gäller till exempel i det ovan refererade exemplet om LifeGene, där Datainspektionen först när projektet var redo att sjösättas invände mot personuppgiftshanteringen i projektet. Nedan exemplifieras Datainspektionens invändningar mot vissa typer av geolokationsspårning i kommunala trådlösa nätverk.

Den ovan refererade danska tillsynsrapporten av dataintrång på flera större statliga myndigheter indikerar att själva valet av arkitektur för ett datasystem

---

fallet Curia C-288/12: ”Court of Justice upholds independence of data protection authorities in case against Hungary” [http://europa.eu/rapid/press-release_MEMO-14-267_en.htm] Ett vidare analogt och välstuderat exempel är mediareglering i EU. Se t ex Kristina Irion, Roxana Radu. ”Delegation to independent regulatory authorities in the media sector: A paradigm shift through the lens of regulatory theory”, 2013. [http://www.ivir.nl/publicaties/download/1136]

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

[31] Centrum för rättvisa. ”Vårdtagare mot Västerbottens läns landsting.” [http://centrumforrattvisa.se/aktuella-fall/vardtagare-mot-vasterbottens-lans-landsting/]; Centrum för rättvisa. ”Centrum för rättvisa mot staten (FRA).” [http://centrumforrattvisa.se/personlig-integritet/centrum-for-rattvisa-tar-fra-lagen-till-europadomstolen/]

[32] 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/]

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

kan låna sig bättre eller sämre till dataskydd. En myndighet med uppdrag att bevaka statens intressen (se ovan) kommer inte att uppmärksamma sådana val av arkitektur, eftersom de skyddar statens intressen givet statens egna val – som naturligtvis innefattar statens val av IT-arkitektur. Datainspektionen skulle, med rätt befogenheter, kunna inta en mer progressiv roll, som inte bara hjälper individer att utöva sina rättigheter givet val som andra redan har gjort, utan också hjälper till exempel staten att göra sådana val som underlättar individens möjligheter att utöva sina rättigheter.

För detta behövs olika verktyg:

Datainspektionen behöver få en möjlighet att följa och delta i tekniska standardiseringsprocesser. Datainspektionen behöver också ges en formell möjlighet att koordinera sådana insatser med andra myndigheter som redan har liknande uppdrag (till exempel Post- och telestyrelsen, se nedan). Nedan återges fyra exempel på sådana processer.

Datainspektionen behöver också tillräckliga personella resurser, både i form av tekniskt och juridiskt kunnande, för att göra positiva bidrag i sådana processer. I Tyskland har vissa dataskyddsmyndigheter (till exempel i Hamburg och Schleswig-Holstein) egna tekniska labb: detta kan vara en modell att plocka upp i Sverige. Datainspektionen i Schleswig-Holstein har till exempel haft tillräckliga resurser och kunnande för att själva kunna bedriva aktiv forskning i EU:s PrimeLife-projekt.[34]

http://www.prime-project.eu

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. Den enda öppningen för deltagande i standardiseringsprocesser som erbjuds dataskyddsmyndigheter i EU-rätten är skäl 66 i direktiv 2009/136/EG, och i Sverige är det Post- och telestyrelsen som är ansvarig för tillsynen av bestämmelserna i detta direktiv. Andra myndigheter, nedan exemplifierade av Energimarknadsinspektionen, ovan exemplifierade av E-delegationen och Digitaliseringskommissionen, skulle kunna arbeta med dataskyddande standardisering men gör inte det. De verksamheter som är ansvariga för teknisk standardisering för myndigheternas räkning har inte i uppdrag att alls ta individers intresse av datasäkerhet i beaktande (jämför Försvarets materielverk eller Försvarets radioanstalt). Det måste anses beklagligt att staten varit snabb att säkerställa konkreta möjligheter att utveckla tekniska förutsättningar för sina ambitioner när det gäller statens egna intressen, men betydligt långsammare och sämre på att utveckla sådana förutsättningar när det gäller individers intressen.

Direktiv 2009/136/EG, skäl 66.

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

[34] Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein, ”PrimeLife - Projektinhalt”. Tillgänglig på: [https://www.datenschutzzentrum.de/projekte/primelife/inhalt/]

integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering (RFID) (2009/387/EG).[35]

...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)[36] eller medlemsländernas satsningar (t ex 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.

http://FIDIS.net

https://abc4trust.eu

http://prisec.kau.se/

I andra standardiseringsprocesser, till exempel Do Not Track-gruppen[37] 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,[38] och EU-kommissionens engagemang var begränsat till ett antal offentliga yttranden från den dåvarande kommissionären.

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 fotnot 36.

...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.[39] Nederländska datainspektionen kom fram till en liknande slutsats i december 2015.[40] Samtidigt har vissa större teknikleverantörer, däribland Apple, experimenterat med ”randomiserade initiala identifierare” (i detta fall MAC-adresser).[41] Då sänder telefonen ut en slumpmässig MAC-adress som byts ut varje gång telefonen kopplar upp sig på nytt till accesspunkterna. Detta

[35] Europeiska unionens officiella tidning. ”KOMMISSIONENS REKOMMENDATION - av den 12 maj 2009 - om genomförandet av principerna om integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering (RFID)” [http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32009H0387&from=EN]

[36] 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]

[37] W3C. ”Tracking Preference Expression (DNT) - W3C Candidate Recommendation 20 August 2015” [https://www.w3.org/TR/tracking-dnt/]

[38] W3C. ”Participants in the Tracking Protection Working Group” [https://www.w3.org/2000/09/dbwg/details?group=49311&public=1]

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

[40] 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]

[41] ”iOS8 MAC Address Randomization Update” [http://blog.mojonetworks.com/ios8-mac-randomgate/]

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.[42] Som ett ”väsentligt krav” på radioutrustning omnämns adekvat skydd för individers rätt till privatliv och dataskydd. Hur man undviker geolokationsspårning av uppkopplade apparater är ett relativt utvecklat forskningsfält[43], och den juridiska och tekniska säkerheten för entreprenörer och tjänsteutvecklare ökar om den tekniska infrastrukturen inte lånar sig för att kringgå Datainspektionens tillsynsbeslut.

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

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[44] 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.[45] 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.

Ei R2015:09

[42] Europeiska unionens officiella tidning. ”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/HTML/?uri=CELEX:32014L0053&from=SV]

[43] Vanhoef, M. Matte, C. Cunche, M. Cardoso, L.S. Piessens, F. ”Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms” [http://papers.mathyvanhoef.com/asiaccs2016.pdf]

[44] 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/]

[45] Broberg, T. Brännlund, R. Kazukauskas, A. Persson, L. Vesterberg, M. ”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]

Tidigare utredningar

Utredningen om tillsyn av den personliga integriteten är inte den första i sitt slag. I kommittéeuppdraget beskrivs ett antal andra utredningar som föreslagit en förstärkning av Datainspektionens tillsynsbefogenheter. Om man bara beaktade sammanställningen i uppdraget finns en risk att man får en missvisande bild av varför tillsynen inte alltid fungerar optimalt idag. Personlig integritet och dataskydd påverkas av en mycket stor mängd statliga utredningar, och det genomgående problemet är att bara sådana utredningar som givits uttryckliga order att begränsa sin uppmärksamhet till dataskydd, uppmärksammar dataskydd.

Dir. 2014:125, s. 4-5.

I E-delegationens slutbetänkande (SOU 2015:66) och samtliga andra skrifter från E-delegationen utgivna sedan 2009[46] lämnas dataskydd och integritet därhän, trots att utredningsuppdraget specifikt klargjort att delegationen bland annat ska överväga hur medborgare kan utöva sina rättigheter. Digitaliseringskommissionens har i sina betänkanden inte heller addresserat dataskydd och integritet.[47]. 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.

Kommittéedirektiv 2009:19, s. 8-9.

Dataskydd.net har sedan juli 2015 arbetat med fyra propositioner, fem statliga utredningar och en myndighetsrapport med inverkan på effektiviteten i integritetsskyddet. Vi har identifierat ytterligare två utredningar, en proposition och en departementespromemoria som vi inte har haft tid att engagera oss i. Dessa finns kartlagda i vår inlaga till Integritetsutredningen Ju 2014:09.[48]

Amelia Andersdotter
Ordförande, Dataskydd.net

[46] E-delegationen. ”Betänkanden” [http://www.edelegationen.se/Publikationer/Betankanden/]

[47] Digitaliseringskommissionen. ”Rapporter” [https://digitaliseringskommissionen.se/rapport/]

[48] Dataskydd.net. ”Inlaga till integritetsutredningen Ju 2014:09”. 1 mars 2016. [https://dataskydd.net/sites/default/files/inlaga_integritetsutredning_dataskyddnet_20160302.pdf]