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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Örsundsbro 2017-11-06

Remissyttrande över integritetskommitténs slutbetänkande – SOU 2017:52

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige. Det här dokumentet är publicerat med licensen CC0.

Sammanfattning av förslag

Sammanfattning.

Tillstyrker förslag: 1, 2, 3, 5, 7, 8, 9, 12, 14, 15, 16, 17, 18, 19, 21, 22, 23, 28, 29, 31, 32, 33, 34, 35.

Tillstyrker delvis förslag: 4, 6, 10, 11, 13, 20, 30, 31, 32.

Avstyrker delvis förslag: 26, 36.

Avstyrker förslag: 24, 25, 27.

Uppförandekoder

Förslag 1, 5. Dataskydd.net är positiva till uppförandekoder, men ser i praktiken hinder för dem på grund av den svenska lagstiftningstekniken på dataskyddsområdet. Registerförfattningarna är uppbyggda så, att de dels definierar en rättslig grund enligt dataskyddsförordningen art. 6.1, men också tar över vissa av de principiella avvägningarna som åligger personuppgiftsansvariga att göra enligt dataskyddsförordningen art. 5. Därtill innehåller en stor andel

registerförfattningar som bestämmer hur en myndighet ska utföra dataskyddsförordningens art. 25 om inbyggt integritetsskydd, och därmed också beskär vad art. 25 betyder för den innevarande myndigheten.

Som vi förstår uppförandekoderna i dataskyddsförordningen art. 40 handlar de om att aktörer inom ett och samma verksamhetsområde ska kunna definiera just principer, standardiserad, lättbegriplig information til konsumenter, och metoder för inbyggt integritetsskydd. Fördelen för aktörerna inom verksamhetsområdet är att de lider mindre risk att låsas in i en föråldrad uppfattning om vad som är ett bra uppförande inom deras verksamhetsfält.

Uppförandekoder skulle därför fungera bättre i ett flexiblare regelverk än det svenska, och ett kort nedslag i det av Integritetskommittén uppmärksammade norska dataskyddsområdet visar att det norska regelverket är enklare än det svenska.[1]

Dataskydd.net har under året konsekvent hävdat att den nuvarande systematiken för registerförfattningar bör ses över. I vår genomgång av Socialdatautredningens betänkande hittade vi till exempel runt 20 uppräkningar på *olika mängder information* som olika verksamheter var förpliktigade att ge privatpersoner vid förfrågan.[2] Om uppförandekoder kan göra något åt sammelsuriet av registerförfattningar är det en bra sak.

Det är redan fallet idag att myndigheter har bättre förutsättning att påverka regeringen och regeringskansliet att förändra registerförfattningarna när myndigheterna känner att de har ett behov av det. Privatpersoner har i sådana lägen mycket få möjligheter att få reda på eller stå emot påverkansförsöken, i den utsträckning de vill det. Uppförandekoder blir en ytterligare sådan nivå.

Viktigt med insyn för säkerhetsfel

Det är mycket viktigt att enskilda privatpersoner och samhället i övrigt får bättre insyn i säkerhetsfel. En fungerande marknad och en fungerande demokratisk stat förutsätter insyn, medvetenhet och valmöjligheter. Idag gör de komplexa värdekedjorna för elektroniska system att orsak och verkan fördunklas: det är för svårt att utan specifik och explicit information få reda på vad som varit problemet, och hur man ska undvika problem.

Både Myndigheten för samhällsskydd och beredskap[3] och Datainspektionen[4] har tyvärr dragit slutsatsen att individer bör berövas insyn och transparens. Vi har bemött myndigheternas felaktiga antaganden i en skrivelse till regeringen tillsammans med föreningen DFRI.[5] Vi hade gärna sett att Integritetskommittén tog starkare spjärn mot ”hemliga hemulen”-betonad myndighetsaktivism.

Rapporter om personuppgiftsincidenter direkt till privatpersoner redan obligatoriska för företag och myndigheter i 47 amerikanska delstater.[6] I åtta av delstaterna publiceras incidentrapporterna direkt på webben för hela världen

Amerikanska delstater med offentligt publicerade incidentrapporter:

- Iowa
  https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/
- Kalifornien
  https://oag.ca.gov/ecrime/databreach/list
- Maryland
  http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx
- Montana
  https://dojmt.gov/consumer/consumers-known-data-breach-incidents/
- New Hampshire
  http://www.doj.nh.gov/consumer/security-breaches/
- Oregon
  https://justice.oregon.gov/consumer/databreach/
- Vermont
  http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-security-breaches/archived-security-breaches.php
- Washington
  http://www.atg.wa.gov/data-breach-notifications

Incidentrapporterna publiceras på Attorney Generals webbplats och går att beskåda av både invånare i delstaten, forskare och andra företag.

Rumänskt sökgränssnitt för offentligt publicerade incidentrapporter:
http://www.dataprotection.ro/notificare/cautari.do

[1] *Se t. ex.* https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/lover-og-regler2/

[2] Dataskydd.net, remissyttrande SOU 2017:66.

[3] MSB, remissyttrande över SOU 2017:36 Informationssäkerhet.

[4] Datainspektionen, *Datainspektionen efterlyser starkare sekretess för incidenter*, 13 juli 2017. Skrivelse till regeringen.

[5] Dataskydd.net och DFRI, skrivelse till regeringen angående Datainspektionens krav på starkare sekretess, 11 oktober 2017.

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

att skåda. Den ekonomiska teorin bakom offentliggörandet är att företag och myndigheter som tvingas stå till svars för sina säkerhetsproblem har starkare incitament att ha goda säkerhetsrutiner och åtgärda säkerhetsproblem som upptäcks.[7] Om det istället är möjligt att hemlighålla säkerhetsproblem kan starka drivkrafter som viljan att slippa ta en kostnad, eller viljan att slippa bli generad, leda företag och myndigheter att inte åtgärda säkerhetsproblemen. Dataskydd.net har beskrivit problemet i ett antal tidigare inlagor och remissyttranden.[8] Transparens kring säkerhetsproblem hjälper företag och myndigheter att förvissa konsumenter och medborgare om att de tar säkerhetsproblem på allvar.[9]

I motsats till den individcentriska incidentrapporteringen finns ingen särskilt väl underbyggd ekonomisk teori bakom EU-ländernas preferenser för incidentrapporter till myndigheter. Betydligt kraftigare ekonomiska sanktioner och mer övervakning av privat sektor skulle, enligt två österrikiska säkerhetsekonomer, behövas för att systemet med incidentrapporter till myndigheter, i syfte att hjälpa myndigheterna utarbeta riktlinjer, ska kunna ha chans att vara effektivt ur säkerhetshöjande perspektiv.[10]

Exempel 1. En risk med att ha en låg nivå av grundinsyn, är att myndigheterna när uppgifter om deras IT-incidenter faktiskt kommer drabbas av mycket negativare uppmärksamhet än vad som är nödvändigt. Dataskydd.net begärde ut incidentrapporter från samtliga myndigheter listade hos Statistiska centralbyrån under våren 2017, och fick då ut en incidentrapport från Moderna muséet, där muséet till följd av en krypteringsattack och bristande säkerhetskopiering tappade sex månaders forskningsdata. I oktober 2017 har Dagens nyheter skrivit om en liknande incident på Myndigheten för press, radio och tv.[11] Om insynen hade varit större och uppmärksamheten kring krypteringsattacker större hade Myndigheten för press, radio och tv personal och ledning varit i mycket bättre ställning att redan tidigare ta tag i säkerhetskopiering.

Exempel 2. Även på andra sätt visar Svenska dagbladets rapporter om IT-säkerhetsincidenter att hemlighållande av incidenterna riskerar att i längden skapa större förtroendeskador för myndigheterna än snabbt offentliggörande.[12] Dataskydd.net erhöll till exempel runt 20 incidentrapporter från Försäkringskassan under våren 2017, som samtliga visade att Försäkringskassan hanterar IT-säkerhetsproblem snabbt och effektivt (inom några timmar).[13] Det är uppenbart att Försäkringskassan skulle kunna vara *ännu bättre*, men de är faktiskt ingen dålig förebild. Eftersom incidentrapporterna hanterats under stort hysch-pysch fick dock Försäkringskassan stark negativ uppmärksamhet när incidenterna väl blev kända: dels blev ju samtliga incidenter kända samtidigt, i stället för att uppdagas efter hand, dels saknas utrymmet i samhället för en balanserad diskussion om vad som är ett acceptabelt sätt att hantera IT-säkerhetsproblem som blir kända.

Hemliga hemulen? Hemulen är en vetenskapligt lagd karaktär, som gillar att studera fenomen omkring och dra slutsatser utifrån deras empiriska tillstånd. Hemulen vet att det saknas anledningar att hålla saker hemliga i onödan. Eftersom det finns så mycket empiriskt stöd för att insyn och transparens har långsiktigt stärkande effekter på IT-säkerhet och informationssäkerhet, kan man se hemulen som en förebild att framhålla i stället för att hålla hemulen hemlig.

Bild: Tarakas, Deviantart.

[7] ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore.

[8] *Se bl. a.* Dataskydd.net:s remissyttrande över SOU 2015:23 om informationssäkerhet, SOU 2017:36 om informationssäkerhet, SOU 2016:41 om dataskydd, och Ju2017/02002/L4 om ett tekniskt sensorsystem.

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

[10] Stefan Laube (University of Münster), Rainer Böhme (University of Innsbruck), The Economics of Mandatory Security Breach Reporting to Authorities, presenterad vid The Workshop on the Economics of Information Security, 22-23 juni 2015 i Delft, Nederländerna.

[11] Dagens nyheter, Svensk myndighet utpressades – betalade lösensumma med skattemedel, 31 oktober 2017.

[12] Svenska dagbladet, Flera allvarliga it-brister hos krismyndigheter, 26 oktober 2017.

[13] Något exempel finns här: `https://dataskydd.net/incidentrapporter-exempel` men kan annars även begäras ut från Försäkringskassan.

Exempel 3. Ett tydligt exempel på hur offentliggörande av incidentrapporter kan göra nytta erfors av Dataskydd.net i mötet med en svensk småföretagare som haft problem med ett litet skript på en server i företagets arbetsmiljö. Skriptet verkade inte utgöra någon fara, men småföretagaren var ändå orolig för att hen borde ha gjort en grundligare utredning. Vi hade emellertid just då tillgång till en incidentrapport från Naturvårdsverket, som haft ett liknande problem under 2016, och kunde dela med oss av Naturvårdsverkets erfarenheter till småföretagaren, som på det sättet fick möjlighet att dels känna att hen *inte var ensam* om att upptäcka små skript, och dels fick en, outförlig men ändock, vägledning till hur man kan undersöka små skript.

Följande historia från det svenska företaget Ericsson, återberättad av Per Göran Ohlsson, Hans Blackman och Jan Svensson, kan tjäna som exempel för vitsen med transparens kring säkerhetsfel:

> Våren 1998 hände något som kunde fått dramatiska konsekvenser för Ericsson och kanske för hela mobiltelefonbranschen. I mitten av maj kom en rapport om att en HotLine Combi den 25 maj hade exploderat i en trädgård i Arlöv. /.../ Samtidigt kom information om en ny explosion i Värmland. /.../
>
> Enligt uppgift ska Ericssonledningen ha tvekat om vad som skulle göras, men Nils Rydbeck krävde att alla telefoner skulle återkallas[. E]n annonskampanj den 31 maj gick ut med budskapet: ”Vi måste få låna din HotLine en stund”.
>
> Ericsson Radios serviceverkstäder hade kvällsöppet till klockan åtta hela följande vecka. Man lödde om litiumbatterier och ökade avståndet mellan batteri och ledare. En kvällstidning lär ha försökt göra reportage med en av de drabbade, men denne vägrade (kanske för att han fått ett nytt golfset som kompensation) och hela historien slutade lyckligt. Ericsson fick stor goodwill för sitt agerande – snabb och effektiv åtgärd utan extra kostnad för kunden och med generösa öppettider. *Det sägs att konkurrenten Mobira (alltså Nokia) anklagade Ericsson för att ha hittat på hela historien för att få publicitet.*
>
> – Ericssons mobiltelefoner 1983–2001, s. 25–26.[14]
>
> [vår italisering]

Tillstyrkta förslag

Utöver vad vi skrivit om uppförandekoder ovan har vi bara ett fåtal kommentarer på de förslag vi anser bra och önskvärda.

Förslag 9 borde eventuellt utökas till att omfatta fler situationer än vård- och omsorg. Beslutsoförmögna har precis som andra enskilda privatpersoner en egen individualitet och identitet som idag är svår att uttrycka i sammanhang där identifiering eller identitetsbekräftelse krävs i elektroniska miljöer. I princip finns inga tekniska förhinder för att en beslutsoförmögen ska kunna tilldelas en egen identitet som sedan exekveras av en förvaltare. Rätten till dataskydd och privatliv innefattar rätten att ha en egen, självständig identitet.

Förslag 22 borde ha kunnat exekveras redan i Ds 2017:26, men bristande uppmärksamhet på regeringskansliet för Integritetskommitténs arbete verkar ha medfört att Finansdepartementet så att säga ”sumpat chansen.”[15]

[14] Per Göran Ohlsson, Hans Blackman och Jan Svensson, Ericssons mobiltelefoner 1983–2001, Roos & Tegnér förlag, 2015. Tryckt i Pozkal, Inowrocław, Polen.

[15] Ds 2017:26, förslag om ändringar i kreditupplysningslagen (KUL), se även Dataskydd.net:s remissyttrande över Ds 2017:26.

Delvis tillstyrkta förslag

Förslag 4 bör på samma sätt som förslag 3 behäftas med ett uppmaning till samverkan mellan Datainspektionen och ansvarig myndighet (i förslagets fall Arbetsmiljöverket).

Förslag 6. Svensk forskning från i höstas visar att integritetsresonemangen på E-hälsomyndigheten har som utgångspunkt att integriteten är någon annans problem.[16] Bland annat präglas organisationen av synen att det är upp till individer själva att hantera integritetsrisker som offentliga IT-satsningar medför.[17] Om det här är en organisationskultur på myndigheten kan det i praktiken bli väldigt svårt för E-hälsomyndigheten att utforma uppförandekoder.

Förslag 10, 11 och 13 är svårbedömda eftersom regeringens politik på området är och lär förbli rörig. Vi har berört frågetecken kring digitaliseringsfrågor i ett tidigare remissyttrande.[18] Kompetenscenter för upphandlingar finns redan, på Kammarkollegiet,[19] Statskontoret[20] och på Statens servicecenter.[21] Även Sveriges kommuner och landsting tillhandahåller en sådan funktion.[22] I oktober fick även Säkerhetspolisen ett utökat uppdrag att tillhandahålla expertis på området.[23] Frågan är om expertisen verkligen blir högre av att man skapar ytterligare ett kompetenscenter.

Det kan noteras att förslag på nationella kompetenscenter för att hantera svårigheter med IT-system har förekommit sedan 1970-talet[24] och att integritetsskyddet ändå blivit sämre än man tänkt, samtidigt som IT-upphandlingarna inte förbättras på det sätt man avsett.

Förslag 20 förefaller redan vara genomfört.[25]

Vad gäller förslaget 30 har vi samma tveksamheter som inför förslagen 10, 11 och 13. Regeringen bör att utredningarna om nya hemliga tvångsmedel[26] samt införandet av nya brottsrubriceringar[27] redan är en sorts reaktion på Riksrevisionens rapport.

---

[16] Peter Johanssons och Sofie Hellbergs, *Att värna personlig integritet – en förutsättning för att nå målen med eHälsa* på s. 95 i Informationssäkerhet och organisationskultur, J. Hallberg, P. Johansson, F. Karlsson, F. Lundberg, B. Lundgren, M. Törner (ed.), Studentlitteratur, september 2017, Lund.

[17] *Ibid.*

[18] Datakydd.net, remissyttrande över SOU 2017:23.

[19] Statens inköpcentral. https://www.kammarkollegiet.se/statens-inkopscentral

[20] *Se t. ex.* http://www.statskontoret.se/forvaltningskultur/kategorisok/?catid=30

[21] Statens SC, konsulttjänster. http://www.statenssc.se/VaraTjanster/Sidor/Ingen%20menyrubrik/Konsulttjanster.aspx

[22] *Se* https://skl.se

[23] Ju2017/08266/PO, Uppdrag till Säkerhetspolisen om fördjupat kunskapsunderlag om arbetet med säkerhetsskydd hos myndigheterna med mest skyddsvärd verksamhet.

[24] SOU 1979:93, ADB och samhällets sårbarhet överväganden och förslag : betänkande, och SOU 1976:69, Teknikupphandling betänkande.

[25] Prop. 2017/18:35, Kontroll av biometriska kännetecken i resehandlingar, Ds 2017:45 En omarbetad utlänningsdatalag – Anpassning till EU:s dataskyddsförordning, *samt* Fi2017/02899/S3, EU:s dataskyddsförordning: Anpassade regler om personuppgiftsbehandling inom skatt, tull och exekution.

[26] Beslagsutredningen (Ju 2016:08) *samt* Utredningen om hemlig dataavläsning (Ju 2016:12).

[27] Bland annat olovlig identitetsanvändning (Proposition 2015/16:150) och förslaget att införa av grovt dataintrång under terrorlagstiftningen (SOU 2017:72).

En huvudsaklig och undanskuffad fråga är därtill i vilken utsträckning IT-brottslagar verkligen kan mildra problemen med samhällets i allmänhet låga IT-säkerhet.[28]

IT-säkerhet och därtill anknuten brottslighet utnyttjar säkerhetsfel som i många fall uppstår, eller inte åtgärdas, för att IT-säkerhet är dyrt och tråkigt. Ett utmärkt exempel är de osäkrade fläktarna i polishuset som Dagens nyheter rapporterade om i artikelserien Det sårbara digitala samhället hösten 2014. Som leverantören av styrsystemen påtalar när DN ringer upp, får man den säkerhet man betalar för.[29]

Många IT-säkerhetsproblem har tyvärr en stark ekonomisk karaktär, inte bara i den mening att det finns de som kan exploatera säkerhetsproblem för egen vinning, utan främst i den mening att det saknas incitament att upprätthålla god IT-säkerhet. I många verksamheter, över allt.[30]

Förslaget 31 har samma problem som förslag 26, nämligen att uppdraget med utredningens formulering riskerar att hamna hos en myndighet som är fundamentalt olämplig för uppdraget. Om målsättningen är att man ska stärka privatpersoners eller företags kompetens på dataskydds- och datasäkerhetsområdena, för dessa aktörers egen skull, måste myndigheten som är ansvarig för utbildningsinsatserna också ha i uppdrag att verka för privatpersoners och företags räkning. Skulle uppdraget till exempel landa hos MSB, är ju MSB:s uppdrag att förbereda *det allmänna* på kriser och krishantering.

Det här gör att MSB, utifrån bara sin uppdragsformulering, inte har särskilt goda förutsättningar att arbeta utifrån det ekonomiska perspektiv vi tror är nödvändigt. En återgång till exemplet med krypteringsattacker är talande: många myndigheter har drabbats av krypteringsattacker enligt MSB:s årssammanställning av incidentrapporter från 2016, men eftersom incidentrapporterna hålls hemliga av MSB får vi ingen bredare allmän diskussion om vilka olika sätt myndigheterna använder för att motverka krypteringsattacker, och vad konsekvenserna blir av att en myndighet inte vidtar säkerhetsåtgärder. Det gör att incidentrapporterna aldrig kommer till någon större allmänutbildande nytta.

Ur *det allmännas* perspektiv kan det givetvis vara befriande att slippa fungera som statuerande exempel på när saker går både bra *och dåligt*, men det kan vara en nödvändig uppoffring för *allmänhetens* bästa. Denna sorts allmänutbildning lånar sig inte MSB till.

Delvis avstyrkta förslag

Förslag 26 är visserligen lovvärt, men frågan är om Myndigheten för samhällsskydd och beredskap (MSB) är en bra myndighet att hantera uppdraget.

[28] *Jfr*. Riksrevisionens genomgångar av informationssäkerhet i offentlig sektor.

[29] Dagens nyheter, IT-expert: Bristerna ett hot mot rikets säkerhet, 3 november 2014.

> *Kjell Carlberg, vd på Kabona, säger till DN att företaget nu ska undersöka säkerheten i sina system. Han pekar på att det finns betydligt fler anordningar som har produkten Webbdatorcentral än de som DN har hittat – och att dessa inte är exponerade mot internet.*
>
> *–Vi kommer informera våra kunder om detta och föreslå dem – om de vill – att fixa så att det inte går att göra detta som ni har gjort. Det är inget problem att lägga detta bakom brandväggar, säger Kjell Carlberg.*

[30] ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore.

Datainspektionen i samband med Konsumentverket, och eventuellt Post- och telestyrelsen bör i stället ha detta uppdrag. Se vidare i avsnittet om avstyrkta förslag.

Förslag 36. Datainspektionen är en fristående och oberoende tillsynsmyndighet för dataskyddslagstiftning i Sverige enligt europeisk rätt. Det gör att det är tveksamt om det verkligen ska flyttas till regeringen att uppdatera vägledningen för integritetsanalys. Det ligger inte heller helt i svensk förvaltningstradition att överlägga implementationen av lagstiftning (så som dataskyddsförordningen) på regeringen.[31]

Avstyrkta förslag

Som vi påtalat i tidigare remissyttranden saknar Myndigheten för samhällsskydd och beredskap (MSB) kompetensen för att utföra de uppdrag som utredningen föreslå att myndigheten ska ansvara för.[32] Vi har i flera remissvar på tidigare och pågående utredningar påpekat att säkerhetsekonomiska frågor förbises i utredningar och lagförslag och att det undergräver konsumenträttigheter och dataskydd.[33] Vi har framhållit att IT-säkerhet inte ska ses framför allt som ett tekniskt problem, utan som ett ekonomiskt. Om det är för lätt och billigt att komma undan med att göra fel, kommer många att göra fel.

Det är för lätt för leverantörer att dölja sina egna misstag för konsumenter och användare, och dessa kan därför inte välja bort leverantörer som inte åtgärdar sina problem. Men inte heller är det förvånande att varken myndigheter eller företag välkomnar ökade insynskrav. Det är aldrig kul att ställas till svars för sina misstag och skulle bli ytterligare en faktor organisationer behöver ta hänsyn till i sin verksamhet, vare sig de konkurrerar om statens resurser eller kunder på en fri marknad. På grund av MSB:s låga förståelse för området, är det olämpligt att MSB får inflytande över privatpersoners informationssäkerhet (förslag 26).

IT-säkerhet är ett marknadsmisslyckande.

Ett marknadsmisslyckade är i neoklassisk och besläktad nationalekonomi en situation där den fria marknaden inte leder till en optimal resursanvändning i samhället. Marknadsmisslyckanden kan uppkomma bland annat på marknader där det finns kollektiva varor, asymmetrisk information, monopol, karteller eller externa effekter.

— Wikipedia.
https://sv.wikipedia.org/wiki/Marknadsmisslyckande

Amelia Andersdotter
Ordförande, Dataskydd.net

[31] SNS, Demokratirådets rapport 2010. Europeiseringen av Sverige.
[32] Dataskydd.net, remissyttrande över SOU 2017:36, SOU 2015:23, skrivelse till regeringen angående Datainspektionens krav på starkare sekretess, samt remissyttrande tillsammans med DFRI över Ju2017/02002/L4.
[33] *Se* https://dataskydd.net/vara-remissvar

Källförteckning

1. Datainspektionen, Dnr. 1704-2017, Vissa frågor om sekretess med anledning av EU:s dataskyddsreform. http://www.datainspektionen.se/Documents/2017-07-13-skrivelse-sekretess.pdf
2. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI), Remissyttrande över promemorian Ju2017/02002/L4 om ett tekniskt sensorsystem hos MSB. https://dataskydd.net/sites/default/files/dfri_dataskyddnet_promemoriaju201702002l4_utan_sig.pdf
3. Deloitte, Deloitte Australian Privacy Index 2015: Transparency is opportunity. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-2015-090516.pdf
4. Ds 2017:26, En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. http://www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2017/06/ds-201726/
5. Ds 2017:45, En omarbetad utlänningsdatalag – Anpassning till EU:s dataskyddsförordning. http://www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2017/10/ds-201745/
6. ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore. https://www.enisa.europa.eu/publications/archive/economics-sec
7. J. Hallberg, P. Johansson, F. Karlsson, F. Lundberg, B. Lundgren, M. Törner (ed.), Informationssäkerhet och organisationskultur, Studentlitteratur, september 2017, Lund.
8. Stefan Laube (University of Münster), Rainer Böhme (University of Innsbruck), The Economics of Mandatory Security Breach Reporting to Authorities, presenterad vid The Workshop on the Economics of Information Security, 22-23 juni 2015 i Delft, Nederländerna. http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf
9. Myndigheten för samhällsskydd och beredskap, remissyttrande över SOU 2017:36. https://aevidentia.files.wordpress.com/2017/07/msb.pdf
10. Per Göran Ohlsson, Hans Blackman och Jan Svensson, Ericssons mobiltelefoner 1983–2001, Roos & Tegnér förlag, 2015. Tryckt i Pozkal, Inowrocław, Polen.
11. Prop. 2017/18:35, Kontroll av biometriska kännetecken i resehandlingar.
12. Regeringen, Fi2017/02899/S3, EU:s dataskyddsförordning: Anpassade regler om personuppgiftsbehandling inom skatt, tull och exekution. http://www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2017/06/eus-dataskyddsforordning-anpassade-regler-om-personuppgiftsbehandling-inom-skatt-tull-och-exekution/
13. Regeringen, Ju2017/08266/PO, Uppdrag till Säkerhetspolisen om fördjupat kunskapsunderlag om arbetet med säkerhetsskydd hos myndigheterna med mest skyddsvärd verksamhet. www.regeringen.se/regeringsuppdrag/2017/10/uppdrag-till-sakerhetspolisen-om-fordjupat-kunskapsunderlag-om-arbetet-med-sakerhetsskydd-hos-myndigheterna-med-mest-skyddsvard-verksamhet/
14. SNS, Demokratirådets rapport 2010. Europeiseringen av Sverige. https://www.sns.se/aktuellt/demokratiradets-rapport-2010-europeiseringen-av-sverige/
15. SOU 1976:69, Teknikupphandling betänkande. http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-7258406
16. SOU 1979:93, ADB och samhällets sårbarhet överväganden och förslag : betänkande. http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-8350833