

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Falun 2017-06-20

Remissyttrande över SOU 2017:23 – digitalförvaltning.nu (Fi2017/01289/DF)

Inledning

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige. Vi har inga synpunkter i sak på hur eller om regeringen väljer att centralisera ansvaret för en digital förvaltning på en myndighet eller flera, men ser ett antal organisatoriska svårigheter och problem som gör att förutsättningarna för bättre dataskydd och integritetsskydd blir försämrade. Vi tror också att den svaga målstyrningen och oklara ambitionerna med digitalisering i dagsläget riskerar att bli till privatpersoners nackdel, i vad gäller privatpersoners möjligheter att utöva sina mänskliga rättigheter dataskydd och privatliv.

Förslag

1. Uppdrag till styrande politiker om precisering av måttstock och mål.

För att en förvaltningsmyndighet, som inte är folkvald och därför inte i princip kan utöva legitim demokratisk makt, ska kunna utföra sitt uppdrag måste dess uppdrag vara tillräckligt väl definierat. Att eftersträva "bästh" känns, enligt Dataskydd.net, inte väl definierat och riskerar att leda till godtyckliga förändringar med stor inverkan på relationen mellan medborgare och stat som inte är demokratiskt förankrade.

Det är inte heller, enligt Dataskydd.net, lyckat att flera på varandra följande utredningar spekulerar i möjligheten att tilldela medborgarna rollen av medarbetare, medverkare eller motsvarande "arbetstagare" i förvaltningsapparaten. Medborgare som inte arbetar i den offentliga förvaltningen gör inte det just för att de inte vill att deras arbetssituation ska dikteras av riksdagen.

2. Utvärdering och uppföljning.

En digitaliseringsmyndighet bör vara ansvarig för att se till att Datatinspektionens riktlinjer om inbyggt integritetskydd används vid genomförandet av risk- och sårbarhetsanalyser inför nya IT-projekt, i enlighet med Dataskyddsförordningens artikel 25.

Digitaliseringsmyndigheten bör också ges en aktiv roll i att kräva konsekvensbedömningar avseende dataskydd enligt Dataskyddsförordningens artikel 35 vid digitaliseringsåtgärder.

Att lösa utvärdering och uppföljning enligt någon annan modell skulle skapa administrativt merarbete och försvåra integrerandet av integritetsaspekter i digitaliseringsprojekt.

Sverige halkar efter?

Dataskydd.net förstår inte mot vilka mätpunkter utredningen håller Sverige när utredningen påstår att Sverige halkar efter i digitalisering.¹ Även om det är ett ofta upprepat påstående att Sverige halkat efter är den enda konkreta skalan mot vilken Sverige har mätts EU-kommissionens så kallade DESI-index.² DESI-indexet har fått genomslag hos till exempel Ekonomistyrningsverket³ men är nyare än regeringens digitaliseringspolitik: konsultföretagen CapGemini, Sogeti, IDC, DTi och RAND Europe utvecklade den första prototypen för ett *benchmarking*-system för EU bara 2011.⁴

Eftersom utredningen inte specificerar att det som idag blivit DESI-indexet som är måttstocken för vad som ska utgöra en svensk framgång, går det inte att göra någon utvärdering av om Sverige verkligen ”halkat efter” i förhållande till tidigare svenska målsättningar.

Dataskydd.net hittar inte heller några hänvisningar till vad det innebär att ”ligga långt fram” i de handlingar som räknas upp av utredningen. Eftersom ”framsteg” och ”utveckling” i viss mån är subjektiva begrepp hade Dataskydd.net gärna sett mer resonemang kring sådana politiska konfliktfrågor som kan och måste uppstå kring prioriteringar i digitaliseringsfrågor.

Medborgarnas maktrelationer i förhållande till staten kan till exempel förändras. Om en medborgare slutar vara ”medborgare”, ”stödtagare” eller ”kund” och istället blir ”medverkare” eller ”medarbetare”⁵ har det konsekvenser för maktrelationen mellan riksdagen och medverkaren i det att medborgaren blir uppdragstagare från riksdagen snarare än att riksdagen blir uppdragstagare från medborgaren. Detta är ingen trivial skillnad av maktbalansen i staten. Det gör skillnad om medborgarna har ett ansvar att logga in på en webbtjänst för att ta reda på staten kommunicerat med medborgarna, eller om staten har ett ansvar att försöka kontakta medborgarna i deras bostad (vilket utredningen föreslår i kapitel 6). I det första fallet måste medborgarna göra en ansträngning för att



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

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

¹SOU 2017:23, kap. 4.1.

²Se t. ex. EU-kommissionens *European Digital Progress Report 2017* om Sverige. <https://ec.europa.eu/digital-single-market/en/scoreboard/sweden>

³Frukostseminarium hos Ekonomistyrningsverket, 17 mars 2017.

⁴Se EU-kommissionens rapport 2011 *eGovernment Benchmarking Pilot on Open Government and Transparency (SMART 2010/0040-2)*, 1 januari 2011.

⁵SOU 2017:23, s. 98.

ta emot kommunikation från staten, i det andra fallet måste staten göra en ansträngning för att komma i kontakt med medborgarna.

Enligt EU-kommissionen har Sverige en mycket god internetinfrastruktur⁶ och ligger långt efter i utvecklingen av datamarknader.⁷ Enligt en OECD-studie kring användning av sociala medier på olika nivåer av styrande i OECD-länderna ligger Sverige tätt efter Storbritannien i Facebook- och Twitter-användning bland de kommunala organen (>80% resp. >90% av kommunerna har sociala media-konton), vilket är långt över det europeiska snittet.⁸ I demokratiutredningens betänkande från 2016⁹ rapporterades att så många som 95% av de svenska kommunerna är aktiva i sociala medier.

Runt hälften av de svenska kommunerna har egna bloggar, vilket enligt studien ser ut att innebära att svenska kommuner är bäst bland kommuner i OECD på att blogga.¹⁰ Sverige har en av världens lägsta nivåer av kontanter i cirkulering,¹¹ med tillhörande höga nivåer av elektroniska betalningar, i förhållande till andra länder. Enligt en annan OECD-studie från 2015 är svenska ungdomar näst bäst i världen på att lägga mycket på internetanvändning efter skolan, svenska kvinnor är näst bäst i världen på att vara olyckliga när de inte har internetuppkoppling, medan svenska unga män är bäst i världen på lägga tid på datorspel.¹²

Samtidigt tog det väldigt lång tid för Sverige att införa till exempel EU:s direktiv om öppna offentliga data från 2003. Faktiskt ända fram till 2009, då den nya offentlighets- och sekretesslagen skrevs. Enligt en artikel författad av Lakomaa och Kallberg, kan det antas ha att göra med det svenska begreppet allmän handling och den svenska offentlighetsprincipen. Eftersom svensk tradition kring offentlighet och vad som ska offentliggöras (beslut fattade av det allmänna, och i lägre utsträckning även beslutsförberedande material) avviker från andra länders traditioner av offentlighet har Sverige andra kostnader och förutsättningar för att genomföra ”öppna data” i enlighet med de definitioner den moderna bemärkelse begreppet använts i internationella organ de senaste 15 åren, än andra länder.¹³

Nu har utredningens uppdrag varit formulerat så, att utredningen inte haft förutsättningar att åtgärda eller ge förslag på hur politikerna ska bli bättre på sitt jobb att utöva ledarskap för både medborgarna och myndigheterna. Utredningen är också en kulmination på flera års kommissioner, kommittéer och delegationer, som likaledes inte kunnat mobilisera sig under något enhetligt politiskt ledarskap. Att utredningen inte fått bättre förhållningsorder från regeringen i sin behandling av digitaliseringsfrågan, för att bland annat förstå vad ”mest”, ”bäst”, ”världsklass” eller ”minst” skulle kunna vara i relation till, ser

⁶Se ovan fotnot 2.

⁷Se EU-kommissionens rapport *European Data Market (SMART 2013/0063) Final Report* från 2017.

⁸Mickoleit, A. (2014), ”Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers”, OECD Working Papers on Public Governance, No. 26, OECD Publishing, Paris.

⁹SOU 2016:5.

¹⁰Se ovan, fotnot 8.

¹¹Arvidsson, Niklas, Jonas Hedman, and Björn Segendorf. ”Cashless Society: When Will Merchants Stop Accepting Cash in Sweden — A Research Model.” i International Workshop on Enterprise Applications and Services in the Finance Industry, pp. 105–113. Springer, Cham, 2016.

¹²OECD (2017), PISA 2015 Results (Volume III): Students’ Well-Being, OECD Publishing, Paris.

¹³Kallberg, J., Lakomaa, E., Institutional Maximization and Path Dependency: The Delay of Implementation of the European Union Public Sector Information Directive in Sweden, i *Journal of e-Democracy and Open Government*, Vol 8 nr 1, 2016.



Perspektiv. Enligt många måttstockar är Sverige redan i världsklass, bäst eller nära toppen av utvecklingen. Alltför otydliga målsättningar och dålig konkretion leder dock till att myndigheter själva tvingas politisera sig för att få rätsida på vad digitaliseringen ska innebära.

vi som ett strukturellt politiskt problem med ledarskap i Sverige där medborgare och konsument är sannolikast att dra kortaste strået.

Nationell digital infrastruktur

Utifrån Dataskydd.net:s perspektiv är det förståeligt varför man inte alltför noggrant vill bestämma på förhand vad en nationell digital infrastruktur skulle kunna vara, men vi oroar oss också för att otydlighet kring detta påverkar både medborgares och konsumenters rättigheter.

Om det inte är uppenbart när en privatperson agerar i egenskap som konsument och när denna agerar i egenskap av medborgare, är det inte säkert att privatpersonen vet hur den ska utkräva ansvar vid fall av fel.

Det som kallas ”nationellt” kan också komma att betraktas som samhällsviktigt, systemviktigt eller samhällskritiskt och kan börja omfattas av begreppet nationell säkerhet. Om digitala infrastrukturer i högre utsträckning, eller godtyckligt, kan börja betecknas som samhällsviktiga eller som att de omfattas av begreppet nationell säkerhet, kan också medborgares och konsumenters möjligheter till ansvarutkrävande i högre utsträckning, eller godtyckligt, minska. Eftersom intresseavvägningen för saker som ses som samhällsviktiga eller viktiga för nationens säkerhet är att nationens intressen går före medborgarens (eller helt enkelt att det ligger i medborgarens intresse att fokus läggs på nationens intresse istället för medborgarens egna intresse) hamnar medborgaren, även när den agerar som konsument, i svagare ställning.

Dataskydd.net har lyft problemet med bristande insyn för konsument och medborgare i digitala infrastrukturer vid ett antal tillfällen.¹⁴

För ett samlat ansvar krävs ett samlat ledarskap

Utredningen föreslår att ansvaret för digitalisering ska samlas under en myndighet, Ekonomistyrningsverket. Dataskydd.net behöver här upprepa problemformuleringarna vi lyfte i yttrandets första avsnitt. Eftersom ”mest”, ”bäst”, ”världsklass” och ”minst” är subjektiva begrepp, och ”digitalisering” i och av sig själv inte heller är särskilt väl definierat, är det många prioriteringar i digitaliseringsprocesser som av nödvändighet kommer att vara politiska. Dessutom anser vi att tillsättandet av flera olika råd¹⁵ och grupper¹⁶, i kombination med att man samtidigt utfärdar en digitaliseringsstrategi som utlovar två nya strategier,¹⁷ ger ett rörligt intryck som inte föranleder känslan av ett samlat ledarskap eller samlat ansvar.

¹⁴ Se bland andra Dataskydd.net, Remissyttrande över SOU 2015:23 – Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten (11.09.2015), Remissyttrande över SOU 2015:39 om en ny myndighetsdatalag (23.11.2015), Inläga till integritetsutredningen Ju 2014:09 från Dataskydd.net (01.03.2016), Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan (25.05.2016), Inläga till utredningen om behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde (kommittédirektiv 2016:63) (21.09.2016), Remissyttrande över promemorian Ju2017/02002/L4 om ett tekniskt sensorsystem hos MSB, tillsammans med DFRI (24.04.2016).

¹⁵ Regeringen (pressrelease 18 april 2016) Regeringen tillsätter råd för digitaliseringen av det offentliga Sverige, Regeringen (pressrelease 10 april 2017) Starkare samordning av digitaliseringspolitiken.

¹⁶ Kommittédirektiv 2017:62, En expertgrupp för digitala investeringar.

¹⁷ För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D).

* POLITISKT ANSVAR ÄR VIKTIGT! *

Digitalisering skapar ett behov av många politiska prioriteringar: budgetar, lagstiftning, verksamhetsramar samt funderingar på hur samhället i grunden ska fungera. Ska medborgarna ta uppdrag från riksdagen, eller agerar riksdagen på medborgarnas uppdrag?

Det vill säga, ska allmänheten tilldelas rollen som medarbetare, arbetstagare eller medverkare i den statliga förvaltningsapparaten, eller även fortsättningsvis kunna förhålla sig passiva i så hög utsträckning som möjligt till de förvaltningsuppdrag som riksdagen anser att det allmänna bör ålägga sig?

Ordningen som utredningen föreslår innebär alltså antingen en politisering av en utförande myndighet, i strid mot den svenska förvaltningstraditionen, eller att Ekonomistyrningsverket döms till ineffektivitet på grund av bristande formell förmåga till att staka ut och agera på sina egna politiska prioriteringar.

I många fall kräver digitaliseringsåtgärder någon sorts lagändringar, vilket märks inte minst på det lagförslag om nya regler för sekretessövergångar som regeringen lämnat på remiss till lagrådet.¹⁸ Betyder det att utredningen föreslår att Ekonomistyrningsverket ska ges uppdraget att lobba regeringen att genomföra lagändringar som myndigheterna själva vill ha för att kunna göra det myndigheterna själva vill uppnå genom en digitaliseringsåtgärd? Utredningen är oklar på den här punkten, men den är givetvis viktig eftersom den ändrar maktbalansen mellan lagstiftarna och utövarna av lagstiftarnas vilja.

Analys, uppföljning, stabsstöd och stöd

Utredningen upprepar vid flera tillfällen att det krävs ett helhetsgrepp om integritet, personuppgiftsskydd och informationssäkerhet.¹⁹ Utredningen listar sedan ett antal dokument, föreskrifter och råd- och samordningsprocesser som den nya centralt ansvariga myndigheten ska utfärda till mottagande myndigheter.²⁰ Men utredningen preciserar inte hur eller ens att dataskydds- och informationssäkerhetsfrågor ska integreras i det arbetet, annat än att det ska ske samordning med Datainspektionen, Myndigheten för samhällsskydd och beredskap (MSB) samt Post- och telestyrelsen.²¹

Det är till exempel inte uppenbart om digitaliseringsmyndighetens expertis, råd, dokument, föreskrifter, analyser och uppföljningar ska komplettera riktlinjer, föreskrifter, råd och uppföljningar om dataskydd och informationssäkerhet, eller om dataskydd och informationssäkerhet ska integreras även i digitaliseringsmyndighetens råd och så vidare.

Inom forskning som betalats av MSB påtalas att bara den senare metoden har någon större utsikt till framgång, det vill säga, dataskydd och informationssäkerhet handlar lika mycket om organisationskultur och att bra tekniska verktyg ställs till personalens förfogande som att det finns riktlinjer och policies.²² Även om detta inte fått genomslag i några föreskrifter från MSB, finns det ingen anledning för regeringen att utfärda ett uppdrag till en ny central myndighet för digitalisering som redan från början är otidsenligt eller stridigt mot vad som i forskning visat sig stämma både internationellt och i Sverige.

Digitaliseringsmyndigheten behöver alltså vara beredd att kopiera, snarare än komplettera, instruktioner från de redan ansvariga myndigheterna på området.

En digitaliseringsmyndighet bör vara ansvarig för att se till att Datainspektionens riktlinjer om inbyggt integritetsskydd²³ används vid genomförandet av risk- och sårbarhetsanalyser inför nya IT-projekt, i enlighet med Dataskyddsförordningens artikel 25.

Digitaliseringsmyndigheten bör också ges en aktiv roll i att kräva konsekvens-

¹⁸Lagrådsremiss, Utökad sekretesskydd i verksamhet för teknisk bearbetning och lagring, 19 maj 2017.

¹⁹SOU 2017:23 s. 14, kap. 4-3.

²⁰SOU 2017:23, kap. 4-5.1, 4-5.3, 4-5.4.

²¹*Ibid.* kap. 4-5.5.

²²Ella Kolkowska och Gurpreet Dhillon, *Organizational power and information security rule compliance*, Computers & Security 33:3-II, 2012.

²³Datainspektionen. Inbyggt integritetsskydd, 2012.

CHECKLISTA FÖR INBYGGT INTEGRITETSSKYDD (genom Datainspektionen):

- ✓ Minimera mängden personuppgifter som lagras i systemet.
- ✓ Använd uppgifter som bara indirekt pekar ut en individ.
- ✓ Ta bort känsliga uppgifter så långt det går.
- ✓ Ersätt namn med pseudonymer.
- ✓ Inte rutinmässigt ha med personnummer som fält.
- ✓ Begränsa åtkomsten till uppgifterna så långt det går.
- ✓ Säker autentisering vid åtkomst.
- ✓ Kryptering överallt, till exempel
 - ▷ Vid lagring av uppgifter.
 - ▷ Vid åtkomst över internet.
 - ▷ Vid åtkomst med mobila enheter.
 - ▷ I databaser.
- ✓ Loggning av åtkomster till uppgifterna.
- ✓ Stöd för säkerhetskopiering.
- ✓ Tydlig behörighetsstyrning.
- ✓ Möjlighet till säker utplåning av uppgifter.
- ✓ Automatiska funktioner för gallring av uppgifter.
- ✓ Logga för att enkelt kunna visa till vilka andra organisationer information har lämnats ut till.
- ✓ Stöd för samtycke och återtagande av samtycke.
- ✓ Funktioner för uppfyllande av förfrågningar om registerutdrag.
- ✓ Ett arbetsflöde som inte uppmuntrar till insamling av fler uppgifter än nödvändigt.
- ✓ Automatisk anonymering innan man använder uppgifter för statistiska skäl.

bedömningar avseende dataskydd enligt Dataskyddsförordningens artikel 35 vid digitaliseringsåtgärder.²⁴

Om det vid digitaliseringen av myndigheternas verksamheter ingår att myndigheterna ska följa gällande lagstiftning även efter digitalisering måste uppföljningsarbetet inkludera sådana aspekter.

Det är vidare fallet att digitaliseringsåtgärder som genomförs utan att man på ett tillräckligt gediget sätt genomfört risk- och sårbarhetsanalys, konsekvensanalyser avseende dataskydd och planering inför dataskydd som standard och som utgångspunkt kan medföra högre kostnader om det visar sig att man senare behöver göra omställningar i systemet till följd av att det första systemet (organisatoriskt eller tekniskt) visade sig vara oförenligt med lagstiftningen.

Vid Örebros universitet har en forskare utvecklat en modern metod för att skapa informationssäkerhetspolicys som bättre överensstämmer med icke försvarsinriktade myndigheters allmänhetsorienterade uppdrag, men som å andra sidan kräver stort engagemang från de som ska vara med och styra och ställa kring myndigheternas verksamheter, digitalisering, IT-verktyg, och informationssäkerhet.²⁵

Dataskydd och IT-säkerhet som inte planeras från början är dyrt och krångligt, för att det är dyrt och krångligt att ändra både bristfälliga IT-system och bristfälliga organisatoriska rutiner.



Amelia Andersdotter

Ordförande, Dataskydd.net

*** INFORMATIONSSÄKERHET ***

“Because of its military and technical origin, information security is sometimes reduced to “the techniques employed to maintain security within a computer system” (Gollmann, 1999). However, information security in the context of organisational governance is much broader. .../ The predominance of the command-and-control approach has a serious consequence when working with employees’ information security behaviours. Employees are still seen as the biggest obstacle to information security. In many cases, their security behaviours are directed by poorly designed information security policies (Stahl et al., 2012). Moreover, most methods focus on changing employees’ behaviours because they consider these behaviours to be irrational and wrong, while the information security policies themselves are “correct” and unchangeable. However, various studies (e.g. Mattia and Dhillon, 2003; Corbin, 2013) have shown that the inability of policy to reflect current work practices is one of the biggest reasons for non-compliance.”

– Ella Kolkowska m.fl., 2017 (se även fotnot 25).

²⁴ Se Dataskydd.net:s förvisso enkla exempel på en konsekvensanalys här: <https://dataskydd.net/file/konsekvensbedomningdataskyddnet201706-05pdf>

²⁵ Ella Kolkowska m. fl., *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method*, Journal of strategic information systems, 6(1) p. 39–57, 2017.

Källförteckning

1. Arvidsson, Niklas, Jonas Hedman, and Björn Segendorf. "Cashless Society: When Will Merchants Stop Accepting Cash in Sweden — A Research Model." i International Workshop on Enterprise Applications and Services in the Finance Industry, pp. 105-113. Springer, Cham, 2016. https://www.researchgate.net/profile/Jonas_Hedman/publication/312569925_Cashless_Society_When_Will_Merchants_Stop_Accepting_Cash_in_Sweden_-_A_Research_Model/links/591197860f7e9bfa06de26e7/Cashless-Society-When-Will-Merchants-Stop-Accepting-Cash-in-Sweden-A-Research-Model.pdf
2. Datainspektionen. Inbyggt integritetsskydd, 2012. <http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/>
3. Ekonomistyrningsverket, Frukostseminarium om digitalisering, 17 mars 2017. <http://www.esv.se/contentassets/f9f5380e56334636a1d3ec45da40122e/frukostseminarium-170317.pdf>
4. EU-kommissionen, 2011 eGovernment Benchmarking Pilot on Open Government and Transparency (SMART 2010/0040-2), 1 januari 2011. <https://ec.europa.eu/digital-single-market/en/news/benchmarking-egovernment-budget-2010-two-studies2011-egovernment-benchmarking-pilot-open>
5. EU-kommissionen, Digital Score Board/European Digital Progress Report 2017, Country: Sweden. <https://ec.europa.eu/digital-single-market/en/scoreboard/sweden>
6. EU-kommissionen, European Data Market (SMART 2013/0063) Final Report, 2 maj 2017. <https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy>
7. Kallberg, J., Lakomaa, E., Institutional Maximization and Path Dependency: The Delay of Implementation of the European Union Public Sector Information Directive in Sweden, i Journal of e-Democracy and Open Government, Vol 8 nr 1, 2016. <http://www.jedem.org/index.php/jedem/article/view/387>
8. Ella Kolkowska m. fl., *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method* Journal of strategic information systems, 6(1) p. 39-57, 2017. <http://oru.diva-portal.org/smash/get/diva2:1058091/FULLTEXT01.pdf>
9. Ella Kolkowska och Gurpreet Dhillon, *Organizational power and information security rule compliance*, Computers & Security 33:3-11, 2012. https://www.researchgate.net/publication/299135936_Organizational_power_and_information_security_rule_compliance
10. Kommittédirektiv 2017:62 En expertgrupp för digitala investeringar. <http://www.regeringen.se/rattsdokument/kommittedirektiv/2017/06/dir.-201762/>
11. Lagrådsremiss, Utökad sekretesskydd i verksamhet för teknisk bearbetning och lagring, 19 maj 2017. <http://www.regeringen.se/rattsdokument/lagradremiss/2017/05/utokat-sekretesskydd-i-verksamhet-for-teknisk-bearbetning-och-lagring/>
12. Mickoleit, A. (2014), "Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers", OECD Working Papers on Public Governance, No. 26, OECD Publishing, Paris. DOI: <http://dx.doi.org/10.1787/5jxrcmgmks-en>
13. OECD (2017), PISA 2015 Results (Volume III): Students' Well-Being, OECD Publishing, Paris. http://www.oecd-ilibrary.org/education/pisa-2015-results-volume-iii_9789264273856-en
14. Regeringen (pressrelease 18 april 2016) Regeringen tillsätter råd för digitaliseringen av det offentliga Sverige. <http://www.regeringen.se/pressmeddelanden/2015/12/regeringen-tillsatter-rad-for-digitaliseringen-av-det-offentliga-sverige/>
15. Regeringen (pressrelease 10 april 2017) Starkare samordning av digitaliseringspolitiken. <http://www.regeringen.se/pressmeddelanden/2017/03/starkare-samordning-av-digitaliseringspolitiken/>
16. Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D). http://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf