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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Enköping 2016-09-21

Inlaga till Dir. 2016:21 — Genomförande av EU:s direktiv om skydd avperson-uppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet

Innehåll

Tidigare utredningar om registerförfattningar 1
Särskilt om särskilda registerförfattningar 2
Personuppgiftsbehandling och EU:s stadga 2
Detaljregler av tekniska lösningar i registerförfattningar 3
Checklistor för inbyggt integritetsskydd 4
Särskilt om information till enskilda. 5
Särskilt om informationssäkerhet 6
Källförteckning 8
Appendix: Skillnad mellan dataskydd och integritet 9

DATASKYDD.NET är en ideell organisation med syfte att verka för informerade beslut om lagstiftning och teknologi i enlighet med de grundläggande rättigheterna till dataskydd och personlig integritet.[1] Den här inlagan är tänkt att bidra till utredningen genom att kartlägga sådana erfarenheter vi har gjort av tidigare statliga utredningar om registerförfattningar, samt verktyg som vi tror att utredningen kan vara betjänta av.

Den här texten går igenom fallgropar i tidigare registerförfattningar som vi hoppas att utredaren kommer att undvika. Den har ett fokus på individens möjligheter till insyn och ansvarsutkrävande som verktyg för myndigheter att höja dataskydd och informationssäkerhet. Sist finns ett appendix om skillnanden mellan integritet och dataskydd.

Tidigare utredningar om registerförfattningar

Dataskydd.net fann det hjälpsamt att utredningen om personuppgiftsbehandling på utlännings- och medborgarskapsområdet[2] förtydligade vilka centrala

[1] https://dataskydd.net/om
[2] SOU 2015:73 Personuppgiftsbehandling på utlännings- och medborgarskapsområdet.

databaser som fanns, och vilka applikationer som användes av olika myndigheter för att komma åt de centrala databaserna. Utmaningen för en privatperson som vill hålla myndigheter ansvariga för beslut, profilering, eller informationssäkerhetsfel är att få reda på hur deras uppgifter flyttas, delas, sprids, säljs och används inom myndigheternas verksamheter.

I integritetskommitténs delbetänkande kapitel 18 är det enda nya bidrag som görs på avsnittets 50 sidor text är två sidor om polisens informationsinhämtning på (det öppna) internet.[3] Effekten av de omfattande och många utredningarna är att staten, trots att den försöker hålla en hög nivå av transparens, istället blir ogenomtränglig för att det inte går att arbeta sig igenom beslutsunderlagen i en tillräckligt snabb takt. Den innevarande utredningen ser ut att ha utmaningen att dess uppdrag delvis överlappar med Kommittédirektiv 2016:73 om RMV och den stundande utvärderingen av domstolsdatalagens första år. Dataskydd.net efterfrågar hänvisningar till, istället för upprepningar av, tidigare utredningars och lagars formuleringar, samt, om möjligt, koordinering med överlappande utredningar.

Särskilt om särskilda registerförfattningar

Som vi kommer tillbaka till (i avsnittet om informationssäkerhet) innebär registerförfattningar att lagstiftaren riskerar att behöva ta över vissa tekniska avvägningar som bäst görs i verksamheterna (se även nedan om inbyggt integritetsskydd). Ju fler speciallagar som finns, desto svårare är det dessutom för privatpersoner att förstå vilka rättigheter de har och hur dessa rättigheter ska utövas. Det är av naturliga skäl mycket svårare för privatpersoner att förhålla sig till hundratals rättighetskataloger än en enda rättighetskatalog. Mot denna bakgrund är det positivt att utredaren fått i uppdrag att lämna förslag till en ny ramlagstiftning.

Personuppgiftsbehandling och EU:s stadga

En konsekvens av direktivet är, så vitt Dataskydd.net förstår, att personuppgiftsbehandling som sker på svenska myndigheter som arbetar med brottsbekämpning, brottmålshantering och straffverkställighet från och med maj 2018 faller under EU:s stadga. Det gör att utredaren även behöver förhålla sig till vad EU-domstolen uttalat i mål som rör artikel 7 och 8 i EU:s stadga, för att kunna garantera att de föreslagna lagändringarna verkligen uppnår ambitionerna i direktivet. I appendixet har Dataskydd.net skisserat en konceptuell skillnad mellan artikel 7 och artikel 8, som vi hoppas är hjälpsam för utredaren. Den är tagen från konceptualiseringen av integritet respektive dataskydd i modern (europeisk) privatlivsforskning.

Det betyder att domstolens utlåtanden i Schrems-målet,[4] Digital Rights Ireland-målet,[5] och det uppkommande Tele2-målet[6] kommer att ha bäring på hur svenska polisen får samla in och till exempel dela personuppgifter med myndigheter i tredje land. Det påverkar vilka möjligheter individer behöver ha tillgång till att ifrågasätta sådan informationsdelning, samt vilka verktyg

[3] SOU 2016:41, kap. 18.7, s. 499-500.
[4] Domslut i Schrems mot Data Protection Commissioner. Mål C-362/14, EU:C:2015:650.
[5] Domslut i de förenade målen C-293/12 och C-594/12, EU:C:2014:238.
[6] Förhandsavgörande i de förenade målen C-203/15 och C-698/15, EU:C:2016:572

tillsynsmyndigheten behöver tilldelas för att kunna effektivt tillse informationsdelningen. Dataskydd.net observerar att tidigare utredningar blandat ihop begreppen ”viss tillsyn”[7] med ”tillräcklig tillsyn”.[8] Den innevarande utredningen är en möjlighet att komma till rätta med begreppsförväxlingen. Det betyder också att stadgans artikel 47, om att privatpersoner har en rätt till ett effektivt rättsmedel inför en opartisk och oavhängig domstol, gäller även för behandling av personuppgifter inom de brottsbekämpande myndigheternas verksamheter, samt att det är EU-domstolens tolkning av innebörden av denna artikel som styr hur den svenska lagstiftningen behöver se ut.

Detaljregler av tekniska lösningar i registerförfattningar

Vissa av de registerförfattningar som utredningen har att ta ställning till innefattar detaljregleringar av vissa tekniska funktioner i användargränssnitt och appliationer. Dataskydd.net motsätter oss förslag om särskilda regler om *sökbegränsningar*[9] och *direktåtkomst*.[10] Dessa invändningar kan kräva särskild uppmärksamhet:

Detaljregler om sökbegränsningar och direktåtkomst innebär en sorts juridisk begränsning för hur användargränssnitt och applikationer kan fungera. Det kan vara lockande ur ett kravspecifikationsperspektiv, men riksdagen ska inte agera upphandlare av mjukvaror utan upprättare av ramverk för myndigheternas verksamheter. Reglerna är onödiga eftersom de begränsar den tekniska utformningen av myndighetens tekniska verktyg, samtidigt som det inte finns några praktiska möjligheter för privatpersoner att säkerställa sig om att reglerna efterlevs.

Vad gäller bestämmelserna i direktivets artikel 19 och 20 tillgodoses de bättre av direktivets allmänt hållna krav i kombination med redovisningskrav, så som transparensloggning, årsredovisningar och incidentrapporter (se nedan). I Sverige ser det ut att vara ett problem att annat elektroniskt överlämnande och utlämnande av uppgifter än direktåtkomst blivit mycket svårt att granska,[11] särskilt för de privatpersoner vars personliga integritet kan ha påverkats (negativt) av över- och utlämningen.

Målet med registerförfattningarna är enligt direktivets ordalydelse att garantera ett starkt skydd för den personliga integriteten, och tillfredsställa privatpersoners möjlighet att utöva sina rättigheter gentemot myndigheterna. För detta syfte är det snarare transparens än detaljreglering som är nödvändig. Det bör vara uppenbart för privatpersoner att, om och hur uppgifter har delats mellan myndigheter vid hanteringen av ett ärende, så att privatpersonen förstår vilka

[7] SOU 2015:31, s. 179.

[8] Förenade målen C-293/12 och C-594/12, EU:C:2014:238, paragraf 68: det är begreppen *fullt ut garanterad* (svenska versionen) och *fully ensured* (engelska versionen) som utredningen i föregående fotnot tolkat som att de innebär att ”vissa möjligheter [för] tillsyn” sammanfaller med.

[9] Dataskydd.net (15 september 2015) Kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag. *samt* Dataskydd.net (30 september 2015) Remissyttrande över SOU 2015:73 om personuppgiftsbehandling på utlännings- och medborgarskapsområdet. *samt* Dataskydd.net (20 oktober 2015) Kommentarer till riksdagen om proposition 2015:16/28 om vissa frågor om behandling av personuppgifter och regleringen av id-kortsverksamheten hos Skatteverket. *samt* Dataskydd.net (23 november 2015) Remissyttrande över SOU 2015:39 om en ny myndighetsdatalag.

[10] Dataskydd.net (30 september 2015) Remissyttrande över SOU 2015:73 om personuppgiftsbehandling på utlännings- och medborgarskapsområdet *samt* Dataskydd.net (23 november 2015) Remissyttrande över SOU 2015:39 om en ny myndighetsdatalag.

[11] Jfr SOU 2015:73 eller Högsta förvaltningsdomstolens dom i mål nr 1356-14.

myndigheter som är inblandade i deras fall. Om det blir lättare för privatpersoner i allmänhet att förstå hur olika myndigheter interagerar för att fatta beslut, kan det också bli lättare för privatpersoner som jobbar på myndigheter att förstå hur myndigheter interagerar för att fatta beslut. Att säkerställa den tekniska säkerheten genom att införa sociala mekanismer för ansvarsutkrävande kan dessutom åtgärda vissa problem med ekonomiska incitament som vi kommer tillbaka till i inlagans sista avsnitt.

Detaljregler om den tekniska utformningen på myndigheternas verktyg riskerar att leda till ett överreglerat system som i praktiken inte skyddar enskildas integritet, är ett dåligt arbetsverktyg och i övrigt missar sina målsättningar. Detta är i linje med vad två på varandra följande Integritetskommittér redan observerat är konsekvensen av statens nuvarande förhållningssätt till integritetsskyddande lagstiftning.[12]

Checklistor för inbyggt integritetsskydd

Enligt skäl 53 och 55 samt artikel 20 i direktivet ska myndigheterna arbeta efter principer om inbyggt integritetsskydd. För många statliga och andra register är det fallet att man inte haft några särskilt strukturerade metoder för att tillgodose integritetsskyddet vid utformningen av arbetsflöden och tekniska system. Detta är en konsekvens av att registerförfattningarna förutsatt en politisk behandling av frågorna, som därför givit förhållandevis goda förutsättningar för särintressen att framhålla vad de tror kommer att vara enklast för dem på kort sikt, samtidigt som privatpersoner inte fått samma möjligheter att delta (både tidsbrist och bristande kunskap bidrar till detta). Att avpolitisera de specifika tekniska kraven som ska ställas på ett system (så långt direktivet tillåter) för att istället politisera vilka möjligheter till ansvarsutkrävande enskilda privatpersoner ska ha, ser alltså rimligt ut för Dataskydd.net.

Utredaren kan utöka både lagstiftarens och allmänhetens förståelse för de nuvarande tekniska förutsättningarna för ansvarsutkrävande genom att gå igenom de uppgiftsbehandlingar som täcks av utredarens uppdrag mot bakgrund av Datainspektionens checklista för inbyggt integritetsskydd från 2012,[13] samt Datainspektionens checklista för säkerhet vid personuppgiftsbehandling från 2008.[14] En sådan genomgång kommer i vilket fall att vara värdefull för utredningen om den avser att ta reda på i vilken utsträckning myndigheterna behöver avvika från denna checklista vid framtida IT-upphandlingar.

I Sverige finns några av Europas ledande experter på transparensloggning vid Karlstad universitet. Inom det europeiska projektet A4Cloud har forskarna på Karlstads universitets PriSec-avdelning bland annat undersökt hur man kan skapa transparens kring dataanvändning i stora IT-system, så som de IT-system som används inom många brottsbekämpande verksamheter. Transparensloggning är ett sätt för medborgarna – de som interagerar med myndigheterna – att förstå hur deras uppgifter flyttar sig mellan olika verksamheter och varför de

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 autenticering 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.

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

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

[14] Datainspektionen, Säkerhet enligt personuppgiftslagen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sakerhet-enligt-personuppgiftslagen/

flyttar sig. Loggningen kan implementeras tekniskt och skapar ett mindre behov än vad som annars skulle finnas av att man i lagstiftning begränsar till exempel hur användargränssnitten för tjänstemännen ska se ut.

Märk särskilt Tobias Pulls avhandling om skydd av integriteten vid transparensloggning.[15] Enligt Pulls är en betydelsefull del av integritetsskyddande loggning (att man skapar ett "spår" över de interaktioner som har skett) att uppgifterna i loggen är *olänkbara* till de privatpersoner som givit upphov till spåren.[16] I avhandlingens sjunde kapitel[17] återknyter Pulls sina transparenta och privatlivsskyddande loggar till sådana projekt för e-handel och molntjänster som Dataskydd.net redan tidigare framhållit: Primelife[18] och A4Cloud.[19]

Särskilt om information till enskilda.

Idag motverkar de brottsbekämpande myndigheterna i Sverige olovlig tillgång till personuppgifter genom dataintrångsbestämmelserna i Brottsbalken. Dataskydd.net är av olika skäl skeptiska till detta förfarande: 1) förfarandet ställer myndigheten i centrum, genom att bara göra det möjligt med ansvarsutkrävande för sådana oförrätter som begåtts mot myndigheten (dess register har kommits åt olovligen), 2) det fråntar privatpersoner att skapa en egen social kultur kring vilken sorts kontroller av deras personuppgifter som är kränkande. Dataskydd.net skulle gärna se att man motverkar olovlig åtkomst, spridning och tillgång till uppgifter genom transparens och insyn mot privatpersoner istället.

För att göra det tydligt när utredningen avviker från direktivets ideologiska huvudmålsättning, anser vi det lämpligt om det framgår i utredningen varför och när man begränsat privatpersoners möjlighet att utkräva ansvar direkt, och vilket resultat man hoppas uppnå med den begränsningen.

För det första vill vi påpeka att det blir lättare för myndigheterna att själva utföra sitt uppdrag på ett informationssäkert sätt ifall de vet varifrån de hämtar uppgifter, när dessa uppgifter hämtas, varför uppgifterna är hämtade och så vidare. Bestämmelserna i direktivets artiklar 13 och 14 bör alltså gå uppfylla bara genom tillräcklig loggning (se avsnittet ovan).

Bestämmelserna i direktivets artikel 24 borde garantera att bestämmelserna i artikel 11 går att uppfylla. Lägg märke till att artikel 11.1 även hänvisar till profilering, en företeelse som hittills i Sverige fått liten uppmärksamhet i svenska statliga utredningar men för vilken det ändå finns någon sorts grund i Integritetskommitténs delbetänkande från i juni 2016,[20] Mediautredningens delbetänkande från november 2015 och Utrikesdepartementets särskilda rapport om algoritmiskt beslutsfattande. EU-domstolen har i ett förhandsavgörande från september 2016 noterat profilering som en särskild risk för enskilda i förhållande till passageraruppgifter.[21] Artikel 12 bör rimligen tolkas som att privatpersoner ska ges möjlighet att få kännedom om, och möjlighet att utkräva ansvar om, de utsatts för en sådan åtgärd.

Incidentrapporter!

Incidentrapporter till privatpersoner enligt direktivets artikel 31 ger privatpersoner egna möjligheter att utkräva ansvar för inträffade IT-säkerhetsfel. Större kännedom och insyn kring IT-säkerhetsproblem skapar bättre förutsättningar att få tillräckliga resurser till nödvändiga investeringar i dataskydds- och informationssäkerhetsåtgärder, samtidigt som det förebygger att de brottsbekämpande myndigheterna blir sittande med en stor andel ouppklarade IT-brott.

Loggning!

Loggning är inte bara ett stöd för myndigheten att veta vad som händer i dess egna IT-system. Loggning kan också användas för att ge medborgare insyn in hur databehandling går till.
Vid uppfyllandet av dataskyddsdirektivets krav på insyn i artikel 13-14 kan det vara särskilt hjälpsamt för myndigheter att hålla koll på vem de sprider uppgifter till, när spridningen skedde samt varifrån de hämtar uppgifter och när de gjorde det.

Årliga rapporter

Årliga rapporter om hur myndigheterna har kommit åt, spridit eller samlat in uppgifter om en enskild privatpersoner hjälper privatpersoner att få kännedom dels om sådant som direktivet ändå förutsätter att de ska få kännedom om, och dels hur de ska utkräva ansvar vid oegentligheter. Att bara årsvis delge informationen tillgodoser också myndigheternas behov av att inte röja utredningar i förtid.

[15] Tobias Pulls. "Preserving Privacy in Transparency Logging", doktorsavhandling, Karlstads universitet, 2015.
[16] Ibid, s. 19.
[17] Ibid, s. 143 ff.
[18] https://www.primelife.eu
[19] https://www.a4cloud.eu
[20] SOU 2016:41, kapitel 11.1.9 och 18.7.
[21] Förhandsavgörande i yttrande 1/5, EU:C:2016:656, paragraf 222–.

De berörda myndigheternas särskilda uppdrag kräver som noteras i artikel 13(3) att information till privatpersoner senareläggs. Dataskydd.net föreslår att utredningen inför en förpliktelse för myndigheterna att varje år skicka ett utdrag till privatpersoner angående sådana åtgärder som listas i artikel 25.1 i direktivet. Det skulle underlätta privatpersoners enga möjligheter att utkräva ansvar för missbruk av åtkomst och tillgång, om än med viss fördröjning. Uppskov från årliga sammanställningar bör tillåtas efter beslut i domstol, till exempel om en privatperson måste utredas under en längre tidsperiod än ett år.

Särskilt om informationssäkerhet

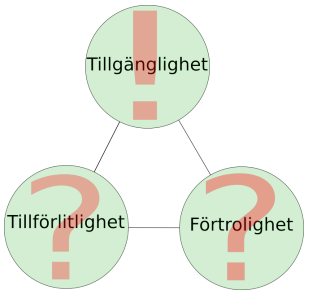
Direktivets artikel 29 listar redan en längre rad kriterier som medlemsländerna måste säkerställa sig om är uppfyllda för varje IT-system. De är lyckligtvis helt förenliga med kraven på inbyggt integritetsskydd i artikel 20. Behovet av ekonomiska incitament för att få bra informationssäkerhet och dataskydd är dock väl etablerat.[22] Vi vill därför ta upp två åtgärder som utredaren kan överväga för att förebygga att brottsbekämpande, brottmålshanterande och straffverkställande myndigheter får otillräckliga incitament att beakta informationssäkerhet.

Transparens mot enskilda är ett sätt att se till att informationssäkerheten hålls hög på myndigheter. Dataskydd.net har förespråkat *individcentrisk incidentrapportering* (det vill säga en bred tolkning av direktivets artikel 31).

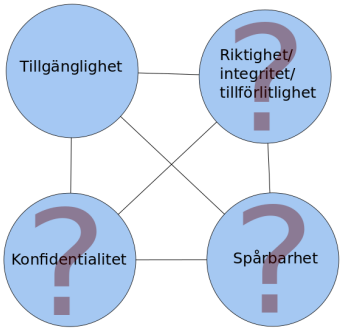
Individcentrisk incidentrapportering finns idag i 47 amerikanska delstater[23] och innebär att enskilda privatpersoner har en rätt att underrättas om IT-säkerhetsproblem som riskerar att ha drabbat dem. Ibland är rättigheten avgränsad till vissa sektorer (till exempel hälso- och sjukvård eller finansindustrin) och ibland är förpliktelserna mer omfattande (till exempel utsträckta även till sociala nätverk, e-postadresser och telefonnummer). Under direktivets bestämmelser kan detta tänkas innefatta rapporter till enskilda då avvikelser inträffat från samtliga eller vissa av kriterierna i artikel 29.2.

Individcentrisk incidentrapportering har givit upphov till tjänster riktade till privatpersoner där de kan utvärdera leverantörer av informationsteknologiska tjänster efter hur väl de hanterar informationssäkerhetsproblem.[24]

Även om kvantitativa studier indikerar att bara ett fåtal individer ställer leverantörer till svars i domstol,[25] finns det marknadsundersökningar som indikerar att konsumenternas förtroende stärks för de leverantörer som berättar för konsumenter när de haft dataläckor och att de även har en strategi för att hantera



Informationssäkerhetsbegrepp i Sverige. I svensk förvaltning används två olika konceptualiseringar av vilka kriterier för säkerhet som är viktiga i IT-miljöer. Dels har vi genom den internationella IT-brottslagstiftningen och dataveten-skapen ärvt en *säkerhetstriad*: tillgänglighet, tillförlitlighet och förtrolighet. Den finns i statliga utredningar om IT-brottsstraffrätt (till exempel SOU 2013:39 om Europarådets IT-brottskonvention).



Å andra sidan har vi också en *säkerhetskvadrupel*, som nämns i NISU-utredningen (SOU 2015:23) och Integritetskommitténs delbetänkande från i somras (SOU 2016:41). Kvadrupeln använder orden tillgänglighet, riktighet, konfidentialitet och spårbarhet.

Till vems fördel begreppen tolkas påverkar maktrelationerna mellan privatpersoner och myndigheter. För myndigheter kan det vara viktigast att uppgifter är tillgängliga, medan det för privatpersoner kan vara viktigare att de är riktiga. Tillgänglighet kan också kollidera med privatpersoners förväntan om förtrolighet. Hårda krav på spårbarhet av privatpersoners nyttjande av e-förvaltningstjänster är inte samma sak som spårbarhet av förvaltningens beslutsprocesser och dataspridning.

[22] *Se* ENISA, Security, Economics and the Internal Market, 2008: "*Information security is now a mainstream political issue, and can no longer be considered the sole purview of technologists. Fortunately, information security economics has recently become a live research topic: as well as collecting data on what fails and how, security economists have discovered that systems often fail not for some technical reason, but because the incentives were wrong. An appropriate regulatory framework is just as important for protecting economic and other activity online as it is offline.*"

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

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

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

dessa.[26] Detta har redan uppmärksammats i ett bidrag till Digitaliseringskommissionen temarapport från juli 2016.[27] Eftersom integritetskommittén redan dragit slutsatsen att de befintliga sanktionerna för integritetsintrång inte har fått den kompensatoriska eller preventiva effekt som har eftersträvats[28] vill vi mena att det just behövs större fokus på privatpersoners möjligheter till ansvarsutkrävande i de svenska registerförfatttningarna.

Den ekonomiska styrningen av myndigheterna från Ekonomistyrningsverket är sådan att det kan vara svårt för myndigheterna att motivera ett gediget dataskydds- och datassäkerhetsarbete om det inte finns ekonomiska konsekvenser av att låta bli att ha ett gediget sådant arbete. Detta märks inte minst på Riksrevisionens återkommande kritik mot myndigheternas IT-säkerhetsarbete.[29]

Här finns en risk att regeringen istället för att skapa förutsättningar för en ekonomistyrningsverksamhet som lämnar utrymme för de brottsbekämpande myndigheterna att investera i IT-säkerhet och dataskydd, istället gör precis ett sådant regelverk som gör det lätt för myndigheterna att under trycket från Ekonomistyrningsverket eftersätta nödvändiga investeringar.

Att de brottsbekämpande myndigheterna kommer att behöva ta stora kostnader för att åtgärda IT-säkerhetsfel är oavsett ekonomistyrningen klar, eftersom en avsaknad av incitament att skapa en bra teknisk infrastruktur ändå kommer att ta sig uttryck i en större andel ouppklarade dataintrång och liknande brottsrubriceringar. De brottsbekämpande myndigheterna tjänar alltså egentligen allra mest på att man i högre utsträckning försöker skapa mekanismer som gör det lätt att komma till bukt med säkerhetsproblemen vid dess tekniska kärna.

Amelia Andersdotter
Ordförande, Dataskydd.net

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

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

[28] SOU 2016:41, Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén., s. 637.

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

Källförteckning

1. Dataskydd.net, Kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag. 15 september 2015. https://dataskydd.net/sites/default/files/domstolsdatalagen_kommentarer_dataskyddnet_ju.pdf
2. Dataskydd.net, Remissyttrande över SOU 2015:73 om personuppgiftsbehandling på utlännings- och medborgarskapsområdet. 30 september 2015. https://dataskydd.net/sites/default/files/sou201573_remissyttrande_dataskyddnet.pdf
3. Dataskydd.net, Kommentarer till riksdagen om proposition 2015:16/28 om vissa frågor om behandling av personuppgifter och regleringen av id-kortsverksamheten hos Skatteverket. 20 oktober 2015. https://dataskydd.net/sites/default/files/dataskyddnet_idregisterkommentar_sku.pdf
4. Dataskydd.net, Remissyttrande över SOU 2015:39 om en ny myndighetsdatalag. 23 november 2015. https://dataskydd.net/sites/default/files/sou201539_remissyttrande_dataskyddnet.pdf
5. 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
6. Digitaliseringskommissionen, Temarapport 2016:1, Det datadrivna samhället. https://digitaliseringskommissionen.se/wp-content/uploads/2013/10/Temarapport-1_Det-datadrivna-samh%C3%A4llet-juni-2016.pdf
7. ENISA, Security, Economics and the Internal Market, 2008. https://www.enisa.europa.eu/publications/archive/economics-sec
8. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679&from=EN
9. Fahriye Seda Gürses, Multilateral Privacy Requirements Analysis in Online Social Network Services, KU Leuven, 2010. https://www.cosic.esat.kuleuven.be/publications/thesis-177.pdf
10. National Conference of State Legislatures. Security Breach Notification Laws. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/7EDG-KVBF].
11. Tobias Pulls. ”Preserving Privacy in Transparency Logging”, doktorsavhandling, Karlstads universitet, 2015. http://www.diva-portal.org/smash/get/diva2:808057/FULLTEXT01.pdf
12. Riksrevisionen. RIR 2007:10 Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen. http://www.riksrevisionen.se/PageFiles/1174/RiR_2007_10.pdf
13. Riksrevionen. RIR 2014:23 Informationssäkerheten i den civila statsförvaltningen. http://www.riksrevisionen.se/PageFiles/20759/RIR_2014_23_infos%C3%A4kerhet_Anpassad.pdf
14. Riksrevisionen. RIR 2016:8 Informationssäkerhetsarbete på nio myndigheter. http://www.riksrevisionen.se/en/rapporter/Rapporter/EFF/2016/Informationssakerhetsarbete-pa-nio-myndigheter/
15. SOU 2007:22 Skyddet för den personliga integriteten - kartläggning och analys. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/03/sou-200722/
16. SOU 2015:39 Myndighetsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/
17. SOU 2015:66 En förvaltning som håller ihop http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/06/sou-201566/
18. SOU 2015:73 Personuppgiftsbehandling på utlännings- och medborgarskapsområdet. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/07/sou-201573/
19. SOU 2016:41 Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/06/sou-201641/

Appendix: Skillnad mellan dataskydd och integritet

EU:S STADGA för grundläggande rättigheter delar till skillnad från andra rättighetsbärande dokument upp den fredade sfären för privatlivet i två separata rättigheter: man har dels en rätt till privatliv och privat sfär (artikel 7) och en rätt till dataskydd (artikel 8). EU-domstolen har framhållit att dessa rättigheter ska tolkas så att artikel 7 i EU:s stadga motsvarar artikel 8.1 i Europeiska konventionen för mänskliga rättigheter.[30] Artikel 8 i EU:s stadga kan istället tolkas som en samling verktyg genom vilka enskilda privatpersoner ges en möjlighet att utöva rätten till privatliv.

Rätten till privatliv, eller rätten till personlig integritet, eller rätten till en egen självständig identitetsutveckling, är flytande begrepp. Rätten till privatliv eller personlig integritet är subjektiv: det är i någon mening upp till varje människa att bestämma vad deras privata sfär är, och det är svårt för varje annan människa att relatera till vad denna första människa bestämt. Utredningen har observerat detta med hänvisningar till Solove och Nissenbaum, och det finns otvetydligen en omfattande doktrin av den rätta - eller breda - förståelsen för termen "integritet" i olika sammanhang. Dataskydd.net har ofta använt sig av den historiska kartläggning av olika privatlivsparadigm som sammanställts av Seda Gürses i hennes datavetenskapliga avhandling vid KU Leuven 2010:[31] 1) Integritet som konfidentalitet: att gömma sig,[32] 2) integritet som kontroll - informationellt självbestämmande,[33] och 3) integritet som praktik - identitetsbildning.[34] Nissenbaum faller under Gürses tredje paradigm. Dataskyddslagstiftningen faller, enligt Gürses, mestadels under det andra paradigmet.

Rätten till dataskydd är inte relativ på samma sätt som rätten till privatliv. Rätten till dataskydd bör ses som en samling metoder som privatpersoner kan använda för att upprätthålla och utöva sin rätt till privatliv.[35] Dessa metoder definieras i lagar så som personuppgiftslagen eller EU:s dataskyddsförordning, men också i registerförfattningar, lagar om hemliga tvångsmedel, och så vidare.

Dataskydd är en självständig och separat rättighet enligt EU:s stadga för grundläggande rättigheter. Denna separata rätighet kan antas ha sin grund i tyska konstitutionsdomstolen resonemang om "informationellt självbestämmande".[36] Politiskt är det möjligt att konkretisera vilka verktyg man anser att rättigheten ska omfatta. Det vill säga, vilka verktyg man vill ge till privatpersoner

[30] WebMindLicenses, C-419/14, EU:C:2015:832, paragraf 70.

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

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

[32] Ibidem, kapitel 2.2.2.

[33] Ibidem, kapitel 2.2.3.

[34] Ibidem, kapitel 2.2.4.

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

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

att utforska sin privata sfär, identitetsutveckling och åsiktsbildning.

Dataskydd är alltså ett enklare begrepp för lagstiftare att arbeta med och förhålla sig till än vad rätten till privatliv är, eftersom dataskydd inte behöver bedömas i varje enskilt fall eller utefter varje enskild individs kontext. Verktygslådan – och det ansvar som tillfaller samhället att effektivt förvalta verktygslåden – möjliggör också att man löser privatlivsproblem som uppstår vid sådana tillfällen då man behöver väga det globala intresset av ett skyddat privatliv mot enskildas intressen av att vara transparenta med sig själva på ett sätt påverkar andra enskilda.[37]

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

> *Today's social, legal, and self-regulatory tools* [*for protecting privacy*] *focus on empowering individuals. They must equally be focused on empowering groups.*
>
> *Individual empowerment is not enough because an individual's disclosure of information about herself impacts many other people. One source of risk is immediate and palpable—information about one person is also information about others.*