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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Socialdepartementet
103 33 Stockholm

Kumla 2016-09-21

Inlaga till Dir. 2016:50 — Dataskyddsförordningen – behandling av personuppgifter och anpassningar av författningar inom Socialdepartementets verksamhetsområde

Innehåll

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 databaser som fanns, och vilka applikationer som användes av olika myndigheter för att komma åt de centrala databaserna. Utmaningen för en privatperson som

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

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.

Detaljregler av tekniska lösningar i registerförfattningar

Dataskydd.net har från början invänt mot detaljreglering av tekniska lösningar som används i myndigheternas verksamheter. Vi motsätter oss förslag om särskilda regler om *sökbegränsningar*[3] och *direktåtkomst*.[4] Vi ser inte heller längre någon poäng med att särskilt reglera att *vilka anställda som behöver ha tillgång* till uppgifter. Att detta ska begränsas till den som verkligen behöver tillgång till uppgifterna följer nämligen av dataskyddsförordningens krav i artikel 25(2)[5] om man inte förutsätter att organisationer anstränger sig för att tolka förordningens bestämmelser till individens nackdel (se även checklistan för inbyggt integritetsskydd på nästa sida). Våra invändningar mot särskilda regler om sökbegränsningar och direktåtkomst 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.

Registerförfattningarna ska, enligt förordningen, garantera privatpersoners rätt till skydd av personuppgifter, och tillfredsställa privatpersoners möjlighet att utöva sina rättigheter gentemot myndigheterna. För att privatpersoner ska kunna utöva sina rättigheter behövs transparens och insyn. 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 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. Dataskydd.net observerar att E-delegationens slutbetänkande noterade att detta inte alltid är fallet.[6]

Detaljregler om den tekniska utformningen på myndigheternas verktyg

[3] 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.

[4] 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.

[5] Art. 25.2 Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

[6] SOU 2015:66, En förvaltning som håller ihop, s. 113-114.

riskerar att leda till ett överreglerat system som i praktiken inte ger ett särskilt starkt skydd för den enskildas integritet. Två på varandra följande Integritetskommittér har redan observerat en sådan konsekvens av statens nuvarande förhållningssätt till integritetsskyddande lagstiftning.[7]

Checklistor för inbyggt integritetsskydd

Utredningsuppdraget berör särskilt behovet av att utredaren återbesöker förslagen från Utredningen om personuppgiftsbehandling vid ISF i betänkandet Inbyggd integritet inom Inspektionen för socialförsäkringen (SOU 2014:67). Inbyggt integritetsskydd blir vid dataskyddsförordningens ikraftträdande i maj 2018 ett juridiskt krav genom förordningens artikel 25.

Dataskydd.net tror att redan det första betänkandet från utredningen hade kunnat förstärkas av att man tidigt i utredningsfasen anammat ett samtidigt tekniskt och juridiskt perspektiv. Den innevarande utredningen skulle kunna förbättra resultatet av den tidigare utredningen genom att gå igenom de uppgiftsbehandlingar som täcks av utredarens uppdrag mot bakgrund av Datainspektionens checklista för inbyggt integritetsskydd från 2012,[8] samt Datainspektionens checklista för säkerhet vid personuppgiftsbehandling från 2008.[9] 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.

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 att samtliga dataskyddsrelaterade beslut måste vara politiska. Det leder i sin tur till förhållandevis goda förutsättningar för särintressen att framhålla för lagstiftaren 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, för att istället politisera vilka möjligheter till ansvarsutkrävande enskilda privatpersoner ska ha, ser alltså rimligt ut för Dataskydd.net.

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 verksamheter under Socialdepartementet. Transparensloggning är ett sätt för medborgarna – de som interagerar med myndigheterna – att förstå hur deras uppgifter flyttar sig mellan olika verksamheter och varför de 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.

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.

[7] 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.

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

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

Märk särskilt Tobias Pulls avhandling om skydd av integriteten vid transparensloggning.[10] 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.[11] I avhandlingens sjunde kapitel[12] återknyter Pulls sina transparenta och privatlivsskyddande loggar till sådana projekt för e-handel och molntjänster som Dataskydd.net redan tidigare framhållit: Primelife[13] och A4Cloud.[14]

Något om informationskraven i Artiklarna 13-19 samt 21-22.

Utredaren har fått i uppdrag att se över i vilken utsträckning myndigheterna behöver ges tillåtelse att avvika från de rättigheter privatpersoner tilldelas i dataskyddsförordningens artikel 13 till 19. Dataskydd.net vill här 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. Det borde alltså ingå i den förhoppningsvis redan etablerade loggningen av myndigheternas användning av IT-stöd att de uppfyller kraven i artiklarna 13 och 14 om dessa loggar görs tillgängliga för medborgarna. Eventuellt kan man fråga om loggarna är tillräckligt begripliga, och hur man i sådana fall kan automatiskt framställa mer lättbegripliga framställningar.

I normalfallet ska myndigheterna heller inte behöva hemlighålla vilka uppgifter de behandlar om privatpersoner (artikel 15). Inte heller är det bra för varken myndigheterna eller privatpersonen om det inte finns en rätt till rättelse (artikel 16). Utredningen om myndighetsdatalag föreslog att försvaga denna rättighet för enskilda, med hänvisning till att myndigheterna tyckte att rättigheten var besvärlig.[15] Det är inget synsätt vi stödjer. Eftersom integritetskommittén redan dragit slutsatsen att de befintliga sanktionerna för integritetsintrång inte har fått den kompensatoriska eller preventiva effekt som har eftersträvats[16] anser vi istället att det snarare krävs mer transparens och insyn, och bättre ansvarsutkrävande. En del i att åtgärda problemen kommittén lyft fram är givetvis ett förstärkt sanktionssystem, men möjligheterna att åberopa sanktionerna behöver också stärkas.

Vid utformningen av ett undantag från rätten att till radering i enlighet med artikel 17.3 c[17] kan det rimligen bara bli tal om att begränsa rättigheten vid till exempel ofrivillig tvångsvård. I fall som rör frivillig vård och kontakter med myndigheter måste man nämligen anta att individen kan göra ett val om den vill ha fortsatt kontakt med myndigheten eller ej. Dataskydd.net har tidigare förespråkat en bredare användning av samtyckeskravet i artikel 6 som bas för privatpersoners interaktioner med myndigheter av den anledningen att samtyc-

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 Dataskyddsförordningens 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.

Veta vad man gör

För att myndigheter ska kunna arbeta med inbyggt integritetsskydd, behöver de till exempel förstå varför vissa uppgifter behövs i deras verksamhet men inte andra. Ett bra sätt att själv förstå varför man behöver kunna använda vissa uppgifter är att kunna förklara det för andra personer, till exempel genom att tillämpa informationskraven i artikel 13-15.

Profilering

Flera viktiga rättigheter i artiklarna 13-15 rör information till privatpersoner om profilering och automatiskt beslutsfattande. Integritetskommittén fastslog att profilering sker på vissa myndigheter inom Socialdepartementets verksamhetsområde i juni 2016. För att privatpersoner ska få en bättre förståelse om och makt över hur myndigheterna använder personuppgifter för att bilda sig uppfattningar om deras karaktärer på algoritmisk väg, krävs att utredningen inte begränsar insynsrättigheterna, eller möjligheterna att invända.

[10] Tobias Pulls. "Preserving Privacy in Transparency Logging", doktorsavhandling, Karlstads universitet, 2015.
[11] Ibid, s. 19.
[12] Ibid, s. 143 ff.
[13] https://www.primelife.eu
[14] https://www.a4cloud.eu
[15] SOU 2015:39, Myndighetsdatalag. s. 556.
[16] SOU 2016:41, Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén., s. 637.
[17] Art 17.3 c: "För skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och i samt artikel 9.3."

keskravet gör det mer tydligt för privatpersoner på vilka premisser de interagerar med myndigheterna. Personuppgifter är inte något som privatpersoner har till låns från myndigheterna, utan någonting som privatpersonerna själva ger upphov till och äger. Genom att frånta individer möjligheten att själva styra över sina personuppgifter, även i sådana fall där staten inte uttryckligen frångtagit individen beslutsrätt, begränsar man denna (allegoriska) upphovsrätt och äganderätt.

Utredningsdirektivet visar en begränsad förståelse för de rättigheter för enskilda som kodifieras i artikel 22 om profilering och automatiskt beslutsfattande. Enligt Integritetskommitténs delbetänkande från i somras används profilering redan vid ett flertal myndigheter, även sådana under Socialdepartementets tillsyn. Till exempel Försäkringskassan.[18] Att begränsa enskildas rättigheter enligt artikel 21 och 22 utgör alltså en hög risk för privatpersonens integritetsskydd, enligt integritetskommitténs bedömning.

Om utredningen därför begränsar privatpersoners rättigheter enligt artikel 21.1 eller enligt artikel 18 med hänvisning till artikel 21.1 försämrar man privatpersoners möjligheter att skydda sig mot sådan profilering som myndigheterna genomför idag.

Kartläggning av personlighetsaspekter och individers vanor sker idag i stor omfattning på internet.[19] Resultaten av sådana kartläggningar används för marknadsföring eller annan beteendepåverkan.[20] Begreppet *nudging* har även fått en politisk innebörd, där kartläggning av individers vanor kan användas för att få individer att bete sig ”korrekt” eller öka individers acceptans för politiska projekt.[21] Man använder ofta beteckningen *profilering* (handlingen att sortera in individer i kategorier baserat på en ”profil” som utgörs av tidigare handlingsmönster, ursprung, identitet, o.s.v.) för att beskriva denna kartläggning.

Profilering kan användas för att påverka privatpersoners känslor[22] eller för att styra politiska kampanjer.[23] Det kan användas för att bestämma vem som statistiskt sett förtjänar att dö,[24] eller vem som inte ska ses som trovärdig vid ansökningar om socialförsäkringar. Personer som har rätt vänner på Facebook kanske kommer undan med fusk i högre utsträckning än personer som har fel vänner på Facebook, beroende på vem som flaggas för granskning. Tidpunkten för det senaste läkarbesöket flaggas som misstänkt

En begränsning av privatpersoners rättigheter enligt artikel 21(1), 18 och 22 skulle alltså medföra sämre skydd för privatpersoner inte bara mot integritetsin-

[18] SOU 2016:41, kapitel 11.1.9.

[19] Mireille Hildebrandt och Serge Gutwirth (red.). Profiling the European Citizen: Cross-Disciplinary Perspectives. Springer Verlag, 2008 *samt* Frederik J. Zuiderveen Borgesius, Improving privacy protection in the area of behavioural targeting, doktorsavhandling, Universiteit van Amsterdam, 2014. Tillgänglig på http://dare.uva.nl/record/1/434236 *samt* Federal Trade Commission, 2016. *Big Data: A Tool for Inclusion or Exclusion?*

[20] Datatilsynet (Norge), 2015. The Great Data Race: How commercial utilisation of personal data challenges privacy.

[21] Paul Rainford och Jane Tinkler. Designing for nudge effects: how behaviour management can ease public sector problems. LSE Research Online, 2011 *samt* Evgeny Morozov. *The Real Privacy Problem.* http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/

[22] Adam D.I. Kramer et al, Experimental evidence of massive-scale emotional contagion through social networks, PNAS, vol 111 nr 24, s. 8788-8790.

[23] Sasha Issenberg. *How Obama Used Big Data to Rally Voters.* https://www.technologyreview.com/s/508836/how-obama-used-big-data-to-rally-voters-part-1/

[24] David Cole (10 maj 2014) ‘We Kill People Based on Metadata’ i New York Review of Books.

trång utan också ett sämre skydd mot *profilering* och *automatisk diskriminering*.

Särskilt om informationssäkerhet

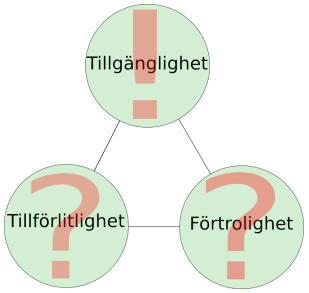
Enligt dataskyddsförordningens artikel 35(10) är det inte tydligt att myndigheter som behandlar personuppgifter med stöd av en registerförfattning måste göra konskvensanalyser och risk- och sårbarhetsanalyser för sina informationsteknologiska system. Istället verkar förordningen förutsätta att lagstiftaren har gjort detta när den arbetade med lagstiftningen. Det är emellertid osannolikt att lagstiftaren har rätt kompetens att utföra ett sådant arbete redan i lagstiftningsprocessen, och bristande risk- och sårbarhetsanalyser hos svenska myndigheter är redan ett stort skäl till att informationssäkerhetsarbete inte fungerar på myndigheterna. Vad utredningen däremot kan göra är att införa tillräckliga ekonomiska incitament för myndigheterna att genomföra risk- och sårbarhetsanalyser på ett sådant sätt att privatpersoners intressen får en central plats. Behovet av ekonomiska incitament för att få bra informationssäkerhet och dataskydd är väl etablerat.[25]

Vi tar här upp två åtgärder som utredaren kan överväga för att förebygga att myndigheterna under Socialdepartementets verksamhetsområde får skeva incitament att tillräckligt beakta informationssäkerhetsåtgärder.

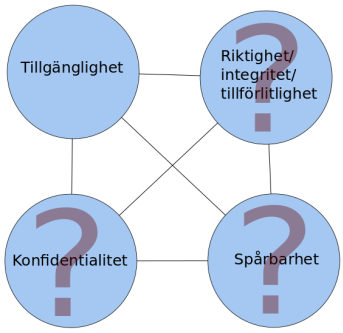
Transparens mot enskilda är ett sätt att se till att informationssäkerheten hålls hög på myndigheter. Dataskydd.net har förespråkat *individcentrisk incidentrapportering* (det vill säga en bred tolkning av dataskyddsförordningens artiklar 33 och 34[26]). En möjlig förstärkning av dataskyddsförordningens regler kan alltså vara att göra incidentrapporterna i artikel 34 tillämpliga för myndigheter i samtliga fall som personuppgiftsincidenter upptäcks.

Individcentrisk incidentrapportering finns idag i 47 amerikanska delstater[27] 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).

Individcentrisk incidentrapportering har givit upphov till tjänster riktade till privatpersoner där de kan utvärdera leverantörer av informationsteknologiska



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.

[25] *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.*"

[26] *Art. 34.1* Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. [*och*] // *Art. 33.3 b* förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas, // *Art. 33.3 c* beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och // *Art. 33.3 d* beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

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

tjänster efter hur väl de hanterar informationssäkerhetsproblem.[28]

Även om kvantitativa studier indikerar att bara ett fåtal individer ställer leverantörer till svars i domstol,[29] 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 dessa.[30] Detta har redan uppmärksammats i ett bidrag till Digitaliseringskommissionen temarapport från juli 2016.[31] Eftersom integritetskommittén redan dragit slutsatsen att de befintliga sanktionerna för integritetsintrång inte har fått den kompensatoriska eller preventiva effekt som har eftersträvats[32] 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.

Här finns en risk att lagstiftaren istället för att skapa förutsättningar för en ekonomistyrningsverksamhet som lämnar utrymme för olika verksamheter inom Socialdepartementets verksamhetsområde, istället gör precis ett sådant regelverk som gör det lätt för myndigheterna att under trycket från Ekonomistyrningsverket eftersätta nödvändiga investeringar. Att emellertid göra medborgarnas förtroende och möjlighet att utkräva ansvar till hårdvaluta, undviker en sådan konsekvens.

Dataskydd.net vill till exempel erinra utredningen om att en allt för stark tilltro till dataintrångsbestämmelsen i Brottsbalken leder till att privatpersoners integritet bara skyddas i den utsträckning myndigheten själv upplever sig vara brottsoffer. Eftersom myndigheten kan välja i vilken utsträckning den blivit utsatt för en kränkning, är paragrafen inget bra ekonomiskt incitament att genomföra tekniska förbättringar, vilket observerades vara en risk med dylika paragrafer i alla fall när de infördes i det internationella regelverket.[33]

Amelia Andersdotter
Ordförande, Dataskydd.net

---

[28] *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/.

[29] *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.

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

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

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

[33] Europarådets rekommendation R 89 (9) om IT-relaterad brottslighet och den därtill hörande slutrapporten från European Committee on Crime Problems. ISBN: 92 – 871 – 1791 – 8. http://www.oas.org/juridico/english/89-9&final%20report.pdf

Källförteckning

1. Frederik J. Zuiderveen Borgesius, Improving privacy protection in the area of behavioural targeting, doktorsavhandling, Universiteit van Amsterdam, 2014. http://dare.uva.nl/record/1/434236
2. 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
3. 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
4. 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
5. Dataskydd.net, Remissyttrande över SOU 2015:39 om en ny myndighetsdatalag. 23 november 2015. https://dataskydd.net/sites/default/files/sou201539_remissyttrande_dataskyddnet.pdf
6. Datatilsynet (Norge), 2015. The Great Data Race: How commercial utilisation of personal data challenges privacy. https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/
7. 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
8. 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
9. ENISA, Security, Economics and the Internal Market, 2008. https://www.enisa.europa.eu/publications/archive/economics-sec
10. 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
11. Europarådets rekommendation R 89 (9) om IT-relaterad brottslighet och den därtill hörande slutrapporten från European Committee on Crime Problems. ISBN: 92 – 871 – 1791 – 8. http://www.oas.org/juridico/english/89-9&final%20report.pdf
12. Federal Trade Commission, 2016. Big Data: A Tool for Inclusion or Exclusion?. https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf
13. 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
14. Adam D.I. Kramer et al, Experimental evidence of massive-scale emotional contagion through social networks, PNAS, vol 111 nr 24, s. 8788-8790. http://www.pnas.org/content/111/24/8788.full.pdf
15. 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].
16. Tobias Pulls. ”Preserving Privacy in Transparency Logging”, doktorsavhandling, Karlstads universitet, 2015. http://www.diva-portal.org/smash/get/diva2:808057/FULLTEXT01.pdf
17. SOU 2007:22 Skyddet för den personliga integriteten - kartläggning och analys. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/03/sou-200722/
18. SOU 2015:39 Myndighetsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/

19. SOU 2015:66 En förvaltning som håller ihop http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/06/sou-201566/

20. SOU 2015:73 Personuppgiftsbehandling på utlännings- och medborgarskapsområdet. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/07/sou-201573/

21. 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.[34] 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:[35] 1) Integritet som konfidentalitet: att gömma sig,[36] 2) integritet som kontroll - informationellt självbestämmande,[37] och 3) integritet som praktik - identitetsbildning.[38] 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.[39] Dessa metoder

[34] 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).*

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

[36] Ibidem, kapitel 2.2.2.

[37] Ibidem, kapitel 2.2.3.

[38] Ibidem, kapitel 2.2.4.

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

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”.[40] Politiskt är det möjligt att konkretisera vilka verktyg man anser att rättigheten ska omfatta. Det vill säga, vilka verktyg man vill ge till privatpersoner 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.[41]

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

[41] *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.*