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 2016-09-23

Inlaga till Dir. 2016:75 — Stärkt integritet i Rättsmedicinalverkets verksamhet

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.

Det innevarande utredningsuppdraget pågår samtidigt som utredningen om genomförandet av EU:s dataskyddsdirektiv om personuppgiftsbehandling i de brottsbekämpande, brottsmålshanterande och straffverkställiga myndigheterna. Denna tidigare utredning ser ut att fått i uppdrag att utreda en ramverkslagstiftning som eventuellt kan komma att täcka Rättsmedicinalverket.[2] Tyvärr har utredningarna inte fått i uppdrag att samarbeta med varandra, vilket kan förvärra splittringen och förvirringen kring integritetsskyddet i svensk lagstiftning.

[1] https://dataskydd.net/om

[2] Kommittédirektiv 2016:21 om genomförande av EU:s direktiv om skydd avpersonuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet.

Tidigare utredningar om registerförfattningar

Dataskydd.net fann det hjälpsamt att utredningen om personuppgiftsbehandling på utlännings- och medborgarskapsområdet[3] 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 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.

Rättsmedicinalverket har dock redan gjort en sådan förteckning i sin rapport Ett nytt författningsstöd för Rättsmedicinalverkets behandling av personuppgifter m.m. (Ju2013/08833/Å). Eftersom förteckningen inte verkar vara tillgänglig på det öppna internet kan det av transparensskäl kanske vara lämpligt att upprepa den även i en statlig utredning, kompletterad med sådana förändringar som kan ha skett de senaste tre åren.

Särskilt om särskilda registerförfattningar

Dataskydd.net uppmuntrar inte särskilda registerförfattningar. Ju fler specialagar om personuppgiftsbehandling som regeringen upprättar, desta svårare blir det för privatpersoner att hålla koll på och utöva sina rättigheter. Det blir också besvärligt för regeringen, departementen och lagstiftaren att hålla reda på vilken lagstiftning som finns och vad den innebär, samtidigt som man ger mycket stort utrymme för den berörda myndigheten att bedriva egenintresserad lobbying. Regeringen har rört sig bort från särskilda registerförfattningar genom att de senaste åren efterfråga en ramlagstiftning för myndigheter,[4] och en ramlagstiftning för myndigheter med brottsbekämpande uppdrag.[5]

Rättsmedicinalverkets egna rapport (Ju2013/08833/Å) anför att en särskild registerförfattning skulle öka verkets ställning hos andra myndigheter, och ge verket tydliga ändamål med personuppgiftsbehandlingarna. Dataskydd.net vill observera att ändamålen normalt ska finnas i regleringsbrevet: det är myndighetens uppdrag som styr vilken sorts personuppgifter som är lämpliga att hantera i verksamheten, och myndigheten ska vid genomförandet av uppdraget beakta principerna om *inbyggt integritetsskydd* och *integritet som standard* (behandlas i ett annat avsnitt). Att andra myndigheter, och inte privatpersoner, får högre förtroende för verket av en registerförfattning är enligt oss inget övertygandeskäl för en specialreglering. Den integritetsskyddande lagstiftning ska ha som mål att ge privatpersoner goda möjligheter att utöva sina stadgefästa mänskliga rättigheter, inte att skapa bra relationer mellan myndigheter.

Enligt oss är det inte heller övertygande att verket inte vill upprätta biträdesavtal: förpliktelserna på personuppgiftsbiträden i EU:s nya dataskyddsförordning är tydliga. Normalt borde verket kunna utveckla ett standardavtal som deras uppdragsgivare får förhålla sig till. Uppdragsgivarna bör också informera sina egna kunder, de vårdade ungdomarna och missbrukarna, om vilka myndigheter som tar del av deras prover och på vilka villkor. Under dataskyddsförordningens

LÄTTBEGRIPLIGT?

Även om det kan vara prestigefyllt att ha en egen lag är det inte säkert att det gör det lättare för privatpersoner att förstå vilka rättigheter de kan utöva mot myndigheten. Det gäller särskilt om myndighetens egna lag tar bort rättigheter från privatpersoner, som rätten att godkänna och få veta vad som händer med uppgifter hos myndigheten. Och oavsett om man specialreglerar eller inte, är det individens känsla av att det är möjligt att få upprättelse vid när fel har begåtts som är det viktiga.

[3] SOU 2015:73 Personuppgiftsbehandling på utlännings- och medborgarskapsområdet.
[4] SOU 2015:39, Myndighetsdatalag med tillhörande kommittédirektiv.
[5] Kommittédirektiv 2016:21 om genomförande av EU:s direktiv om skydd avpersonuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet.

artiklar 13.1 e[6] och 4.1.9[7] ser det ändå ut som att patienterna har en rätt att få reda på detta.

Dataskydd.net skulle föredra, med anledning av utredningens uppdrag att undersöka behovet av särskilda registerförfattningar för allt fler register, att utredaren prioriterar bättre förutsättningar för privatpersoner att hålla myndigheterna ansvariga för hur de utövar sina befogenheter mot bakgrunden av en ramverkslagstiftning samtidigt som myndigheterna får anledning att följa föreskrifter, rekommendationer och checklistor från Datainspektionen vid investeringar i nya IT-system. Detta är ämnet i de tre följande avsnitten.

PRINCIPER OCH UPPFÖLJNING

Istället för att politiskt etablera vad kravspecifikationen på ett tekniskt system ska vara, bör de politiska diskussionerna vara fokuserade på hur lätt det ska vara för privatpersoner att förstå och granska vad de tekniska systemen till sist gör. Dessutom behövs riktiga mekanismer för ansvarsutkrävande, till exempel att myndigheter inte kan dra på sig rättegångskostnader i miljonklassen för att skrämma privatpersoner från att inte utkräva ansvar för felaktigheter (exempel från Integritetskommitténs delbetänkande kapitel 23).

Detaljregler av tekniska lösningar i registerförfattningar

Dataskydd.net har ofta invänt mot detaljreglering av tekniska lösningar som används i myndigheternas verksamheter. Vi motsätter oss förslag om särskilda regler om *sökbegränsningar*[8] och *direktåtkomst.*[9] 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 principer i artikel 5.1 d (uppgiftsminimering) och förtydligandet i artikel 25(2) att tekniska och organisatoriska åtgärder ska vidtas för att begränsa uppgifternas tillgänglighet till vad som är nödvändigt. Även om Rättsmedicinalverkets verksamhet skulle finnas täckas av EU:s dataskyddsdirektiv i viss utsträckning, gäller även där att artikel 29 redan medför obligatoriska åtkomstbegränsningar. 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.

Som Rättsmedicinalverket observerar skickar de ofta uppgifter till svenska

[6] Art. 13.1 e: ”Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:” /.../ ”e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.”

[7] Art. 4.1.9 ”*mottagare:* en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte[.]”

[8] 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.

[9] 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.

och utländska över okrypterad e-post, vilket räknas eom elektroniskt utlämnande av annat slag än direktåtkomst och därför ändå inte skulle falla under teknisk detaljreglering. Dataskydd.net kan på bara anekdotisk grund nämna åtminstone tre verktyg som verket skulle kunna använda för att lösa sitt problem med säkert informationsutlämnande: Deaddrop (utvecklat av svenska Sysctl), OpenPGP (verktyg för e-postkryptering) och SpiderOak (utvecklat av amerikanska SpiderOak). Säkerligen har myndigheternas och verkens professionella IT-avdelningar och deras underleverantörer ännu fler erfarenheter av sådana verktyg som kan användas för att tillgodo se både dataskydd och informationssäkerhet. Vi kommer i det avslutande avsnittet återkomma till problemet för både integriteten som för säkerheten är att det fram till EU:s dataskyddsförordning ser ut att ha saknats möjligheter till vettig ekonomistyrning av myndigheternas IT-satsningar. Om de ekonomiska incitamenten att utreda organisatoriska och tekniska förändringar till säkerhetens och integritetens fördel, kommer en registerförfattning med tekniska detaljregler inte att kompensera för det uteblivna skyddet.

Målet med registerförfattningarna är 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 insyn och ansvarsutkrävande som behövs än detaljreglering. 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 ärende. De måste också ges möjligheter att effektivt hålla myndigheter till svars som inte vidtar lämpliga åtgärder eller som genomför olovliga behandlingar.

Detaljregler om den tekniska utformningen på myndigheternas verktyg riskerar att leda till ett överreglerat system som i praktiken inte ger ett särskilt starkt skydd för den enskildas integritet. Rättsmedicinalverket verkar godta detta genom att i sin rapport skriva att en dedicerad registerförfattning innebär fördelar för verket och för andra myndigheter. Man fortsätter i sådana fall på den linje som två på varandra följande Integritetskommittér observerat ger ett mindre tillfredsställande integritetsskydd än vad lagstiftaren ser ut att ha avsett.[10]

Ekonomiska incitament

Bristande ekonomiska incitament att ta dataskydd och integritet, men även säkerhet, på allvar är ett lika stort problem på myndigheter som det är i näringslivet. Med transparens- och insynsåtgärder som transparensloggning, incidentrapporter och samtycke inför nya åtgärder ökar man konsekvenserna för myndigheten att inte utreda tekniska lösningar på tekniska problem, eftersom fler privatpersoner då förstår om eller att de borde klaga.

Checklistor för inbyggt integritetsskydd

För många statliga verksamheter, och uppenbarligen också för Rättsmedicinalverket, 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, för att istället politisera vilka möjligheter till ansvarsutkrävande enskilda privatpersoner ska ha, ser alltså rimligt ut för Dataskydd.net.

[10] 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.

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,[11] samt Datainspektionens checklista för säkerhet vid personuppgiftsbehandling från 2008.[12] 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 utbildningsväsendet. Transparensloggning är ett sätt för medborgarna – de som interagerar med myndigheterna – att förstå hur deras uppgifter flyttar sig mellan olika verksamheter och varför förflyttningen sker. 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. På grund av dataskyddsförordningens delade ansvar mellan personuppgiftsbiträden och personuppgiftsombud kan man också tänka sig att det naturligt kommer att uppstå en ordning där de stora uppgiftsmottagarna (till exempel SCB) i högre utsträckning ansvarar även för små uppgiftsöverlämnares (till exempel studiecirklars) transparensloggning.

Märk särskilt Tobias Pulls avhandling om skydd av integriteten vid transparensloggning.[13] 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.[14] I avhandlingens sjunde kapitel[15] återknyter Pulls sina transparenta och privatlivsskyddande loggar till sådana projekt för e-handel och molntjänster som Dataskydd.net redan tidigare framhållit: Primelife[16] och A4Cloud.[17]

Särskilt om information till enskilda.

Utredaren har inte fått i uppdrag att se över hur det kan bli mer begripligt för enskilda privatpersoner vilka register de hamnar i, eller hur och i vilken utsträckning olika myndigheter samarbetar med Rättsmedicinalverket. Eftersom det är oklart huruvida Rättsmedicinalverket helt eller delvis kommer att påverkas av EU:s dataskyddsdirektiv eller EU:s dataskyddsförordning, är det inte klart för Dataskydd.net vilken sorts informationskrav till individer som kommer bli gällande för Rättsmedicinalverket.

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.

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

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

[13] Tobias Pulls. "Preserving Privacy in Transparency Logging", doktorsavhandling, Karlstads universitet, 2015.

[14] Ibid, s. 19.

[15] Ibid, s. 143 ff.

[16] https://www.primelife.eu

[17] https://www.a4cloud.eu

För privatpersoner är det förmodligen bättre att dataskyddsförordningens informationskrav i artiklarna 13-14 tillämpas än att informationskraven i dataskyddsdirektivets artiklar 12-13 tillämpas. Att ge privatpersoner bättre rätt borde dock inte vara något problem då Rättsmedicinalverket hittills stött sig på personuppgiftslagen för sin personuppgiftsbehandling.

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 (dataskyddsförordningen) om dessa loggar görs tillgängliga för privatpersoner på ett begripligt sätt. I normalfallet ska myndigheter inte behöva hemlighålla vilka uppgifter de behandlar om privatpersoner (artikel 15, dataskyddsförordningen). Inte heller är det bra för varken myndigheterna eller privatpersonen om det inte finns en rätt till rättelse (artikel 16, dataskyddsförordningen). Vi kommer nedan även att ta upp incidentrapportering (artikel 34, dataskyddsförordningen) som ett rimligt och lämpligt verktyg för insyn och ansvarsutkrävande.

Samtyckeskravet i dataskyddsförordningens artikel 6.1 a fyller oftast funktionen av att uppmärksamma privatpersoner på att någonting förändrats från sitt tidigare tillstånd (i kombination med principen om ändamålsbegränsning). Dels kräver samtycket att privatpersonen informeras, så att samma person kan ta ställning, dels ger det privatpersonen egen makt att säga nej. Även vid sådana tillfällen då Rättsmedicinalverket behöver förlita sig på den juridiska basen i artikel 6.1 c eller 6.1 e är det dock viktigt att man inte eftersätter även kontinuerliga uppdateringar till privatpersonen om vem dess ärende faktiskt hanteras av. Dataskydd.net tror att meddelanden riktade direkt mot berörda privatpersoner läses i högre utsträckning än svensk författningssamling, och att sådana meddelanden om ändamålsändring eller spridning därför kan vara mer effektiva för att hålla privatpersoner underrättade.

Forskning och statistik

Rättsmedicinalverket lämnar ut många av sina uppgifter om privatpersoner till forskare, och bedriver även egen utveckling. Dessutom genomför myndigheten statistisk behandling av uppgifter. Den här sortens uppgiftsutlämningar bör meddelas privatpersoner, och om utlämningen är mycket omfattande kan myndigheterna istället skicka årliga sammanställningar av antalet utlämnanden som skett. Det ger en liten men ändå inte obefintlig möjlighet till ansvarsutkrävande för privatpersoner och skyddar deras rättigheter och friheter.

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 informationstekniska 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. Behovet av ekonomiska incitament för att få bra informationssäkerhet och dataskydd är däremot väl etablerat.[18]

Vi tar här upp två åtgärder som utredaren kan överväga för att förebygga att myndigheter i utbildningsväsendet får otillräckliga incitament att beakta

[18] *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.*"

informationssäkerhet.

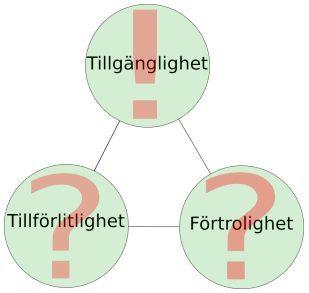
Transparens mot enskilda är ett sätt att se till att informationssäkerheten hålls hög på myndigheter. Dataskydd.net har förespråkat *individcentrisk incidentrapportering* (det vill säga en bred tolkning av dataskyddsförordningens artiklar 33 och 34[19]). En möjlig förstärkning av dataskyddsförordningens 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[20] 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).

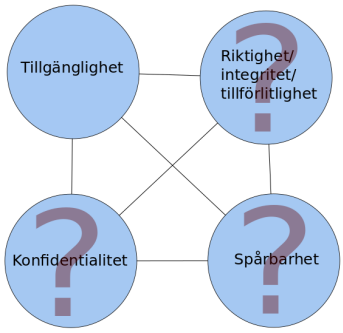
Individcentrisk incidentrapportering har givit upphov till tjänster riktade till privatpersoner där de kan utvärdera leverantörer av informationsteknologiska tjänster efter hur väl de hanterar informationssäkerhetsproblem.[21]

Även om kvantitativa studier indikerar att bara ett fåtal individer ställer leverantörer till svars i domstol,[22] 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.[23] Detta har redan uppmärksammats i ett bidrag till Digitaliseringskommissionen temarapport från juli 2016.[24]

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. Om man, när man gör fel, inte lider risk att bli upptäckt, inte kan ställas till svars annat än genom ett ledset brev från Datainspektionen, och privatpersonerna vars integritet man kränker är



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.

[19] *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.

Art. 34.2 Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone [*följande*] upplysningar och åtgärder[:]

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.

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

[21] *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/.

[22] *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.

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

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

förbehållna att skriva brev till riksdagen i förhoppningen om att en registerförfattning ska ändras, då är man förmodligen inte så pepp på att tänka den extra vändan om vilka tekniska skyddsåtgärder som är rimliga. Särskilt inte om man redan sitter på gamla system som i många fall inte uppfyller ens grundläggande krav på dataskyddande, transparensinriktade databehandlingar.

Här finns en risk att regeringen istället för att skapa förutsättningar för en ekonomistyrningsverksamhet som lämnar utrymme för Rättsmedicinalverket 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. Av särskild oro för Dataskydd.net är att de pågående utredningarna för personuppgiftshantering på myndigheter väljer samma typ av modell för ansvarsutkrävande som föreslogs i utredningen Myndighetsdatalag (SOU 2015:39), eftersom denna utredning dels reducerade omfattningen av de dåligt upprätthållna rättigheter privatpersoner redan har och begränsade Datainspektionens möjligheter att invända mot felaktiga behandlingar på ett kraftfullt sätt.

Eftersom integritetskommittén redan dragit slutsatsen att de befintliga sanktionerna för integritetsintrång inte har fått den kompensatoriska eller preventiva effekt som har eftersträvats[25] vill vi mena att det just behövs större fokus på privatpersoners möjligheter till ansvarsutkrävande i de svenska registerförfattningarna. Datainspektionens roll bör inte heller försvagas visavi myndigheterna. Sannolikt behövs även högre skadestånd, och begränsade möjligheter för myndigheterna att ådra sig höga rättegångskostnader, men sådana förändringar ligger utanför den innevarande utredningen och Dataskydd.net har istället kontakter med Integritetskommittén om sådana övervägningar.

Dataskydd.net tror följdaktligen att man kan se hela dataskyddskomplexet som ett likaledes moraliskt som juridiskt ramverk, men att dess förutsättningar att fungera så beror på hur utredaren råder lagstiftaren att tillämpa dess principer.

Amelia Andersdotter
Ordförande, Dataskydd.net

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

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. Rättsmedicinalverket, Ett nytt författningsstöd för Rättsmedicinalverkets behandling av personuppgifter m.m. (Ju2013/08833/Å).
13. SOU 2007:22 Skyddet för den personliga integriteten - kartläggning och analys. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/03/sou-200722/
14. SOU 2015:39 Myndighetsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/
15. SOU 2015:66 En förvaltning som håller ihop http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/06/sou-201566/
16. SOU 2015:73 Personuppgiftsbehandling på utlännings- och medborgarskapsområdet. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/07/sou-201573/
17. 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.[26] 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:[27] 1) Integritet som konfidentalitet: att gömma sig,[28] 2) integritet som kontroll - informationellt självbestämmande,[29] och 3) integritet som praktik - identitetsbildning.[30] 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.[31] 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".[32] 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

[26] 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).*

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

[28] Ibidem, kapitel 2.2.2.

[29] Ibidem, kapitel 2.2.3.

[30] Ibidem, kapitel 2.2.4.

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

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

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.[33]

[33] *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.*