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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Socialdepartementet
103 33 Stockholm

Enköping 2016-09-21

Inlaga till Dir. 2016:63 — Personuppgiftsbehandling inom utbildningsområdet

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 principer i artikel 5.1 d (uppgiftsminimering) och förtydligande 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.

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 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 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]

[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.

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. 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.[7]

Särskilt om särskilda registerförfattningar

Som vi kommer tillbaka till i det sista 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 för privatpersoner att förstå vilka rättigheter de har och hur dessa rättigheter ska utövas. Istället för att skapa en rättighetskatalog per register behövs allmänna principer för prövning av rimligheten i varje registrering, tror vi.

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. Vi återkommer till detta i de tre följande avsnitten.

Checklistor för 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, för att istället politisera vilka möjligheter till ansvarsutkrävande enskilda privatpersoner ska ha, ser alltså rimligt ut för Dataskydd.net.

Den svenska lagstiftaren och de svenska myndigheterna sitter nu i positionen att den europeiska lagstiftaren redan i princip bestämt vilka möjligheter till ansvarsutkrävande som är möjliga. Utredaren kan alltså bara föreslå försämringar eller förbättringar av privatpersoners möjlighet till ansvarsutkrävande enligt förordningen. 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,[8] samt Datainspektionens checklista för säkerhet vid personuppgiftsbe-

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/

handling 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.

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.[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]

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 hamnas i och flyttas mellan under en livstid. Eftersom bättre möjligheter för ansvarsutkrävande för privatpersoner och bättre insyn i uppgiftshantering för privatpersoner är dataskyddsförordningens kärnvärden anser vi dock att det är motiverat att särskilt beröra kraven i artiklarna 13-22 här.

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. 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 privatpersoner på ett begripligt sätt. I normalfallet ska myndigheter inte behöva hemlighålla vilka uppgifter de behandlar om privatpersoner (artikel 15). Inte heller är det bra för varken

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.

Gallring!

En viktig rättighet för privatpersoner att kunna utkräva ansvar. Att kontinuerligt underhålla sin förståelse för vilka myndigheter som samlar på sig och har samlat på sig uppgifter om den egna personen är en omöjlig ansträngning, vilket begränsar privatpersoners möjligheter att utkräva ansvar. Om registrena har bra och säkra gallrings- och utplåningsrutiner behöver inte privatpersoner konstant underhålla sin förståelse för allt fler register och deras författningar.

Forskning och statistik

Som utredningsdirektiven påtalar är det många register i utbildningsväsendet som används för statistikframställning, och som kan användas till underlag för forskning. Integritetskommittén kom i sitt betänkande i juni 2016 fram till att statistisk databehandling är oöverskådlig, och att forskning är en allvarlig risk för integriteten. Avidentifiering av arkiverade uppgifter är ett sätt att minska risken. Att ge människor möjlighet att samtycke till att forskas på är ett annat.

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

[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

myndigheterna eller privatpersonen om det inte finns en rätt till rättelse (artikel 16). Vi kommer nedan även att ta upp incidentrapportering (förordningens artikel 34) som ett rimligt och lämpligt verktyg för insyn.

Dataskydd.net har tidigare förespråkat en bredare användning av samtyckeskravet i artikel 6 som bas för privatpersoners interaktioner med myndigheter av den anledningen att samtyckeskravet gör det mer tydligt för privatpersoner på vilka premisser de interagerar med myndigheterna. Samtycke kan till exempel användas inför överföringar av uppgifterna till andra myndigheter, verksamheter eller företag – då slipper individen det kontinuerliga uppdraget att begära registerutdrag och information för att få veta hur uppgifterna spridits, eller om de verkligen gallrats.

Försäljning av personuppgifter eller annan utlämning av personuppgifter från myndigheter i utbildningsväsendet till reklamföretag är en annan aspekt utredningen har att beakta. Myndigheter i utbildningsväsendet tidigare har kunnat lämna ut och sälja personuppgifter till reklamföretag med hänvisning till intresseavvägningar och berättigat intressen, men nu inte längre kommer kunna göra det på grund av dataskyddsförordningen 6.1 f. Dataskydd.net rekommenderar starkt emot att man inför specialregler som möjliggör ytterligare försäljning och utlämning av personuppgifter till kommersiell verksamhet utan individens samtycke. 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 frångått individen beslutsrätt, begränsar man denna (allegoriska) upphovsrätt och äganderätt.

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.[15]

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

Transparens mot enskilda är ett sätt att se till att informationssäkerheten

[15] *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.*"

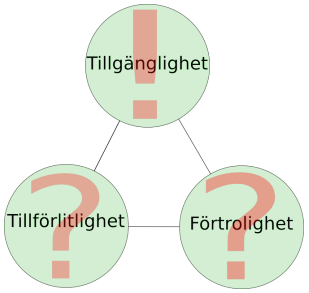
hålls hög på myndigheter. Dataskydd.net har förespråkat *individcentrisk incidentrapportering* (det vill säga en bred tolkning av dataskyddsförordningens artiklar 33 och 34[16]). En möjlig förstärkning av dataskyddsförordningens regler kan alltså vara att göra incidentrapporterna i artikel 34 tillämpliga för myndigheter i samtliga fall som personuppgiftsincidenter upptäcks.

Individcentrisk incidentrapportering finns idag i 47 amerikanska delstater[17] 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).

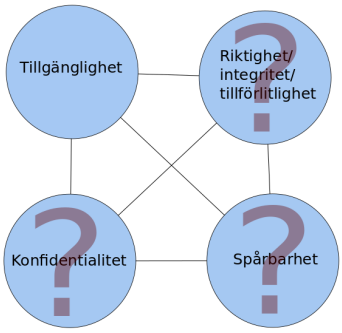
Individcentrisk incidentrapportering har givit upphov till tjänster riktade till privatpersoner där de kan utvärdera leverantörer av informationsteknologiska tjänster efter hur väl de hanterar informationssäkerhetsproblem.[18]

Även om kvantitativa studier indikerar att bara ett fåtal individer ställer leverantörer till svars i domstol,[19] 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.[20] Detta har redan uppmärksammats i ett bidrag till Digitaliseringskommissionen temarapport från juli 2016.[21] Eftersom integritetskommittén redan dragit slutsatsen att de befintliga sanktionerna för integritetsintrång inte har fått den kompensatoriska eller preventiva effekt som har eftersträvats[22] 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 Riks-



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 datavetenskapen 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.

[16] *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.

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

[18] *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/.

[19] *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.

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

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

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

revisionens återkommande kritik mot myndigheternas IT-säkerhetsarbete,[23] men också till exempel på Datainspektionens kritik av kommunernas satsningar på molntjänster i skolan. De flesta utbildningsrelaterade verksamheter kommer i praktiken att vara beroende i sina IT-satsningar av företag som utvecklar IT-stöd för utbildningsverk, som även de arbetar under ekonomiska incitament.

Här finns en risk att regeringen istället för att skapa förutsättningar för en ekonomistyrningsverksamhet som lämnar utrymme för olika verksamheter inom utbildningsområdet 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. När det saknas ekonomiska incitament för teknisk säkerhet, träder därutöver brottsbalkens juridiska skyddsmekanismer för tekniska system i kraft, vilket kan få till följd att skolans underleverantörer drar skolans elever inför rätta.[24] Man fråga sig om det verkligen är en lyckad moralisk fostran att elever inte får vara dumma mot skolans underleverantörers datorer, samtidigt som det saknas konsekvenser för underleverantören av att ha haft ett osäkert system och eleverna i fråga inte behövde ta ansvar för eventuella negativa konsekvenser deras agerande hade för skolan och andra elever.

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 tillämpar dess principer inom utbildningsområdet.

Amelia Andersdotter
Ordförande, Dataskydd.net

[23] 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.

[24] Se dom i Falu tingsrätt i mål nr B 1520-13, avkunnad 9 september 2013.

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.[25] 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:[26] 1) Integritet som konfidentalitet: att gömma sig,[27] 2) integritet som kontroll - informationellt självbestämmande,[28] och 3) integritet som praktik - identitetsbildning.[29] 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.[30] 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".[31] Politiskt är det möjligt att konkretisera vilka verktyg man anser att rättigheten ska omfatta. Det vill säga, vilka verktyg man vill ge till privatpersoner

[25] 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).*

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

[27] Ibidem, kapitel 2.2.2.

[28] Ibidem, kapitel 2.2.3.

[29] Ibidem, kapitel 2.2.4.

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

[31] 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.[32]

[32] *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.*