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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Falun 2017-07-10

Remissyttrande över SOU 2017:29 – Brottsdatalag

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige. Nedan följer en sammanställning av våra förslag till ändringar i föreslagen Brottsdatalag och Brottsdataförordning. Denna sammanställning består bara av de konkreta förändringar vi vill se i lagtexten så som föreslagen av utredningar. Efter förslagssammanställningen följer förklaringar till var och en av förslagen. Vi försöker i huvudsak hålla oss till den systematik som etablerats i betänkandet, men när det har visat sig svårt eller olämpligt indikerar vi hur vi avviker. En källförteckning med webblänkar till de referenser för vilka sådana finns, går att finna längst bak i remissyttrandet.

Som övergripande observation vill vi nämna att det är synd att utredaren inte noggrannare läst Integritetskommitténs delbetänkande från förra sommaren. Vi tror att två på varandra följande (med tio års mellanrum) riksdagskommittér med uppdrag att stärka den personliga integriteten har funnit att integritetsskyddet i Sverige inte fungerar tillfredsställande eftersom riksdagskommittéernas arbete huvudsakligen varit frånkopplat den utredande verksamhet som leder till lagstifnting på dataskyddsområdet.

Förslag

Onödig avgränsning av lagens tillämpningsområde (Brottsdatalag 1 kap. 4 §)
— Den föreslagna avgränsningen i Brottsdatalag 1 kap. 4 § bör tas bort. Se vidare s. 3. — Brottsdatalag 4 kap. 6 § 1 stycket kompletteras med texten ”, om inte den registrerades intresse av att kunna utöva sina rättigheter väger tyngre än myndighetens intresse av att inte lämna ut informationen.” Se vidare s. 3 och s. 19.
Biometriska uppgifter (Brottsdatalag 1 kap. 6 §).
— Begreppet *biometriska uppgifter* bör definieras som ”personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, och som möjliggör eller bekräftar unik identifiering av personen i fråga.” Se vidare s. 4.
Profilering och krav på transparens (Brottsdatalag 1 kap. 6 § och 4 kap. 4 §).
— Begreppet *profilering* bör definieras som ”behandling av personuppgifter som består i att dessa används för att bedöma personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga aspekter rörande dennas

arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar." Se vidare s. 4.

— Begreppet *överföring* bör definieras som "behandling av personuppgifter på ett sätt som innebär att uppgifterna skickas, vidarebefodras, förmedlas eller på annat sätt görs tillgängliga för någon i ett tredje land." Se vidare s. 18 och s. 4.

— Till Brottsdatalag 4 kap. 4 § tillfogas meningen "Myndigheten ska också lämna information om profilering som genomförts eller genomförs mot den enskilde, eller mot kategorier av enskilda som den enskilde tillhör, även om sådan profilering bara har lett till manuella beslut och även då sådan profilering använts inom ramen för kontrollverksamhet som senare lett till brottsutredning." Se vidare s. 4 och s. 7.

Pseudonymisering, diarieföring och arkivering (Brottsdatalag 1 kap. 6 §, 2 kap. 2 § och 2 kap. 5 §).

— Begreppet *pseudonymisering* bör definieras som "behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person." Se vidare s. 4.

— Till Brottsdatalag 2 kap. 2 § tillfogas meningen "Uppgifterna ska pseudonymiseras om inte detta vore uppenbarligen orimligt eller förhindra vidare handläggning av ärendet." Se vidare s. 4 och s. 7.

— Till Brottsdatalag 2 kap. 5 § tillfogas meningen "Uppgifterna ska pseudonymiseras om det inte finns särskilda skäl till varför detta vore olämpligt." Se vidare s. 4 och s. 7.

Personuppgiftsbiträden, inbyggt integritetskydd och dataskyddsprinciper (Brottsdatalag 3 kap. 3 § och 3 kap. 20 §).

— Brottsdatalag 3 kap. 20 § ändras till lydelsen "Det som sägs om den personuppgiftsansvariges skyldigheter i 3, 5, 6, 8 och 12 §§ gäller även för personuppgiftsbiträden." Se vidare s. 7.

Oklar relevans av tillsynsbestämmelsen i Brottsdatalag 5 kap. 6 §.

— Brottsdatalag 5 kap. 6 § tas bort. Se vidare s. 10.
— Hänvisning i Brottsdatalag 5 kap. 7 § 1 stycket 1 punkten till 5 kap. 6 § tas bort. Se vidare s. 10.
— Hänvisning i Brottsdataförordning 5 kap. 4 § byts från att peka på Brottsdatalag 5 kap. 6 § till att peka på Brottsdatalag 5 kap. 4 § (förhandssamråd). Se vidare s. 10.
— Brottsdatalag 5 kap. 7 § 2 stycket kompletteras med texten "Förelägganden kan förenas med vite." Se vidare s. 15 och s. 10.
— Det bör förtydligas att rätten till överklagande som anges i 7 kap. 4 § också gäller privatpersoner som drabbas av tillsynsmyndighetens beslut. Se vidare s. 10.

Omotiverade begränsningar av sanktionerade handlingar (Brottsdatalag 6 kap. 1 §).

— Brottsdatalag 6 kap. 1 § 1 stycket kompletteras med punkten "4. 4 kap. 1-4 §§ samt 9-10 §§." Se vidare s. 15.
— Brottsdatalag 6 kap 1 § 1 stycket punkt 2 kompletteras med "3 kap. 12 §" och "3 kap. 17-18 §§". Se vidare s. 15.

Storleken på de administrativa avgifterna är inte adekvata (Brottsdatalag 6 kap. 3 §).

— Brottsdatalag 6 kap. 3 § 1 stycket ändras så att anvisningen till högstabeloppet för sanktionsavgiften sätts till 1 % av myndighetens eller verksamhetens årsomsättning. Se vidare s. 15.
— Brottsdatalag 6 kap. 3 § 2 stycket ändras så att anvisningen till högstabeloppet för sanktionsavgiften sätts till 2 % av myndighetens eller verksamhetens årsomsättning. Se vidare s. 15.

Enskildas rätt till insyn (Brottsdatalag 3 kap. 9 § och Brottsdataförordning 9 §).

— Brottsdataförordningen 3 kap. 9 § kompletteras med texten ”Tillsynsmyndigheten ska underhålla en lista med sådana databehandlingssystem eller verksamheter för vilka privatpersoner inte kan erhålla information om personuppgiftsincidenter. Verksamheter ska föranmäla sin avsikt att klassa ett visst system som allt för viktigt för riket för att privatpersoner ska kunna få veta när det skett personuppgiftsincidenter i systemet.” Se vidare s. 19.
— Brottsdatalag 3 kap. 10 § 1 stycket ändras till ”Om en personuppgiftsincident som ska anmälas enligt 9 § första stycket *har inträffat,* ska den personuppgiftsansvarige *som huvudregel* utan onödigt dröjsmål underrätta den registrerade om incidenten.” Se vidare s. 19.
— I Brottsdatalag 4 kap. 2 § tas orden ”i specifika fall” bort, eftersom de inte bidrar till klarhet kring vad de ytterligare informationsförpliktelserna är menade att uppnå. Se vidare s. 19.
— Brottsdatalag 4 kap. 11 § tas bort. Paragrafen tillför ingenting till 4 kap. 9-10 §§. Se vidare s. 19.

Information och överskottsinformation från hemliga tvångsmedel.

— Vi föreslår att det preciseras att Brottsdatalag ska tillämpas även på information och överskottsinformation som insamlats av brottsbekämpande myndigheter genom användning av hemliga tvångsmedel. Se vidare s. 21.

Allmän struktur (kommentarer på kap. 6, 7)

Dataskydd.net tillstyrker förslaget att det behövs en ny lagstiftning[1] och att denna ska vara av generellt tillämplig men subsidiär karaktär.[2] Vi tillstyrker även förslaget att lagen med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom EU ska upphävas.[3]

Vi är därtill tveksamma över nyttan med speciallagstiftning så som polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, skattebrottdatalagen, tullbrottsdatalagen och domstolsdatalagen, eftersom vi tror att medborgare enklare kan förhålla sig till sammanhållna krav som är samlade i *en* lag.[4] Det följer av detta av vi också vänder oss emot att även fortsättningsvis försöka hantera den veritabla myriad av samarbeten mellan brottsbekämpande myndigheter i syfte att stävja terrorism i särskilda registerförfattningar[5], eller av att särreglera Säkerhetspolisens eller polisens verksamheter i de delar som gäller nationell säkerhet.[6]

Kraven på ändamålsbegränsning, dokumentation, och upplysningar till enskilda samt tillsynsmyndigheten som föreslås i Brottsdatalag borde vara tillräckliga för att varje verksamhet ska kunna samla in och behandla de uppgifter som krävs för deras verksamhet, och bör i samband med de tekniska och organisatoriska kraven som föreslår i Brottsdatalag med tillhörande förordning redan kunnas göra tillräckliga för att privatpersoner ska kunna utöva sina rättigheter och tillsynsmyndigheten utöva ändamålsenlig tillsyn (se även föreslagen Brottsdatalag 2 kap. 1 §).

Vi tillstyrker därmed förslagen i kap. 7.1.1-7.1.5,[7] med det förbehållet till förslaget i kapitel 7.1.3 att vi inte anser att *informationssäkerhet* bör ges samma status som *nationell säkerhet*,[8] utan att även *informationssäkerhet* bör täckas

[1] SOU 2017:29, kap. 6.1.1.
[2] *Ibid*., kap. 6.1.2.
[3] *Ibid*., kap. 6.1.4
[4] *Jfr*. ibid., s. 141.
[5] Jfr Dataskydd.net:s remissyttrande på Ds 2016:31.
[6] SOU 2017:29, kap. 7.2.1.
[7] *Ibid*., kap. 7.1.1-7.1.5
[8] *Jfr*. *ibid*., s. 169 samt förslag i samma utredning kap. 7.2.1.

av Brottsdatalag i den utsträckning bevakningen eller övervakningen görs med avsikt att upptäcka brottsliga förfaranden. Vi noterar också att friskrivningarna från de rättigheter som enskild ska åtnjuta (det vill säga tillfällen då dessa inte ska gå att utöva eller kunna nekas av behörig myndighet) enligt den föreslagna Brottsdatalag 4 kap. är så generösa att det inte kan finnas något problem att integrera även Säkerhetspolisens och polisens skyldigheter vad gäller nationell säkerhet under lagens allmänna tillämpningsområde.[9]

Dataskydd.net har tidigare påtalat att den ökade normaliseringen av IT-stöd och internettillgång hos den svenska befolkningen, konsumentbasen, hos företag och på myndigheter medför ett behov av att även säkerhetslagstiftningen i samhället klarar av att hantera informationssäkerhetsproblem som normalföreteelser snarare än som samhällskriser.[10] Övervakning och bevakning som sker i syfte att förebygga brotten företagsspionage, intrång i företagshemlighet eller dataintrång, och som genomförs av därtill behörig myndighet bör alltså falla under Brottsdatalag på samma sätt som övervakning och bevakning som sker i syfte att förebygga andra brott gör det.

Till sist är det olyckligt att utredningen lägger sådan vikt vid att lagen ska gälla för behandling av sådana uppgifter som är helt eller delvis automatiserad. Lagen kan inte utgöra något fullgott skydd för fysiska personers fri- och rättigheter ifall dataskyddsintrång blir lovligt eller oreglerat så fort någon använder papper och penna i stället för dator. Den i media uppmärksammade *svarta bok* som upprättats av banken Nordea,[11] eller det likaledes uppmärksammade *kvinnoregistret* som upprättats hos polisen i Stockholm,[12] visar att både allmänheten och medier förväntar sig att skyddet för personuppgifter ska täcka även handskrivet klotter, i den utsträckning sådant klotter på något sätt gör intrång i enskilds privatliv eller dataskydd, eller kränker dennes identitet.

Vi föreslår en ändring i Brottsdatalag 4 kap. 6 § 1 stycket för att myndigheter inte ska kunna hålla sådana icke-automatiserade behandlingar hemliga för berörda privatpersoner eller organisationer som representerar dessa privatpersoner.

Sammanfattning.

Tillstyrker: 6.1.1, 6.1.2, 6.1.4, 7.1.1, 7.1.2, 7.1.4, 7.1.5, 7.3.

Avstyrker delvis: 7.1.3.

Avstyrker: 7.1.6, 7.2.1.

Brottsdatalag 1 kap. 4 § enligt förslaget bör tas bort. Det finns ingen anledning att i den svenska nationella lagstiftningen införa ett särskilt undantag från dataskyddet för den sortens utredningsarbete som beskrivs i den föreslagna paragrafen.

Brottsdatalag 4 kap. 6 § 1 stycket kompletteras med texten ”, om inte den registrades intresse av att kunna utöva sina rättigheterväger tyngre än myndighetens intresse av att inte lämna ut informationen.”

[9] *Ibid.*, kap. 7.2.1.
[10] Se Dataskydd.net:s remissyttranden över SOU 2015:23 och SOU 2015:25.
[11] *Se t. ex.* Svenska dagbladet (17 februari 2015) Nordea bluffade om hemliga kundregistret.
[12] *Se t. ex.* Sveriges radios temasajt Kvinnoregistret http://sverigesradio.se/kvinnoregistret/

Angående definitioner (kap. 6.2)

Utredningen vill hävda att en biometrisk uppgift bara skulle vara en sådan uppgift som tagits fram genom särskild teknisk behandling,[13] och att man därför ska införa en definition som inte innehåller uppräkningen med exempel på biometriska uppgifter som EU:s lagstiftare hjälpsamt tillfört direktivet för att underlätta tolkningen i medlemsländerna.

Möjligen har utredaren förvirrats av att bokstavsdefinitionen av biometri (”*vetenskapsgren som studerar biologiska fenomen med statistiska metoder*”)[14] för tankarna till datorer, eftersom statistiska beräkningar har blivit enklare att genomföra i större skala efter datorns inträde i vetenskapen. Det borde dock vara rätt klart att biometriska uppgifter inte ska definieras som enbart resultatet av en teknisk (i praktiken datoriserad) behandling.[15]

En biometrisk uppgift är en uppgift om någonting mätbart hos en privatperson, till exempel dess fysiska utseende (avstånd mellan ögonen, hårfärg, hur långt ringfingret är i förhållande till långfingret och dylika uppgifter). I EU:s lagstiftning om biometriska pass anges till exempel att biometriska uppgifter är fingeravtryck och fotografier.[16] I Integritetskommitténs delbetänkande från juni 2016 beskrivs biometriska uppgifter som ett samlingsnamn för egenskaper och beteenden som går att mäta.[17] Om något går att mäta kan man göra statistik av det. Till exempel lär 89% av finska befolkningen ha blå ögon, medan bara 1,2% av den tunisiska befolkningen har blå ögon.[18]

Utredningens definition skulle innebära att alla former av insamling av biometriska uppgifter undantas från det särskilt starka skydd som EU:s lagstiftare verkar ha tänkt sig.[19]

Ett ytterligare förbiseende från utredningen är beslutet att inte införa någon definition av eller särskilda regler för transparens kring profilering.[20]

En möjlig förklaring, som utredningen inte själv anför, är att utredaren anser att profilering bara innebär problem för privatpersoner i frågor om skyddet och utövandet av deras rättigheter när det gäller sådana kontrollåtgärder som utredningen diskuterar i kapitel 8.2.10.[21] Integritetskommittén hittade till exempel under sommaren 2016 att vissa myndigheter med kontrolluppdrag ägnade sig åt profilering för att kunna rikta sina mer närgående granskningar mer effektivt[22] och har föreslagit att åtgärder vidtas för att reglera profilering i sitt betänkande från juni 2017.[23]

Det är emellertid inte svårt att föreställa sig att profilering används även inom

Livspusslet. Profilering kan utgöra en del av en beslutsprocess eller kontrollverksamhet varigenom myndigheter med hjälp av dator går igenom många små pusselbitar från en privatpersons liv, som denna kanske inte själv är medveten om att den givit upphov till eller som kanske är så avknoppade från sin kontext att de är irrelevanta. Datorn bestämmer sedan om man baserat på det fullständiga pusslet som den lagt utifrån databitarna vilken kategori av människor man statistiskt sett tillhör. Man kan ge datorn (eller egentligen algoritmen, via ingångsvärdena) instruktioner för vad som ska anses vara ”normalt”.

Bild: Hans Splinter, CC-BY-ND, 12 januari 2012, Flickr.

[13] SOU 2017:29, s. 149.

[14] Nationalencyklopedins ordbok, första bandet (A-HZ), Språkdata, Göteborg och Bokförlaget Bra Böcker AB, Höganäs, 1995.

[15] Möjligheten finns så klart att man med teknisk behandling menar sådan uppgift som tillkommit medelst någon form av teknik, men i sådana fall skulle fotografier, som ju är resultatet av att man tillämpar fotograferingsteknik, täckas av definitionen i strid mot vad utredaren anför är syftet med utredaren underliga avgränsning.

[16] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna (som ändrat av förordning 444/2009 den 28 maj 2009).

[17] SOU 2016:41, s. 583.

[18] Se https://sv.wikipedia.org/wiki/%C3%96gonf%C3%A4rg_hos_m%C3%A4nniskan

[19] Direktiv 680/2016, Art. 10.

[20] SOU 2017:29, s. 147.

[21] SOU 2017:29, kap. 8.2.10.

[22] SOU 2016:41, kap. 11.1.9.

[23] SOU 2017:52, kap. 8.2.3.

de brottsbekämpande myndigheterna (även om det med nuvarande lagstiftning vore svårt för Dataskydd.net att bevisa att sådan profilering ägt rum). Det uppmärksammade *romregistret* i Skåne[24] var till exempel av sådan karaktär att individer som utmärkte sig genom en viss egenskap (de var romer) blev registrerade för att denna egenskapen antogs föranleda högre risk att de därför skulle besitta oönskvärda egenskaper (så som att vara kriminella). Man kan tänka sig ett antal mer eller mindre liknande situationer: en grupp med personer befinner sig ofta utanför en viss fritidsgård och antas därför vara inblandade i brottslighet, en person med viss frisyr antas ha intresse för en särskild sorts rusningsmedel, på grund av att en Facebook-användare börjat följa vissa sidor på Facebook har en så kallad klusteralgoritm[25] som används i sociala medier-bevakande syfte fått för sig att man är i riskzonen för att ägna sig åt bidragsbrott, och så vidare.

Bestämmelserna i direktivets artikel 11 är menade att skapa förutsägbarhet kring denna sorts profilerande verksamhet, både för tillsynsmyndigheten och för privatpersoner. Utredarens förslag realiserar dock inte det skyddet som den europeiska lagstiftaren har tänkt sig, eftersom profilering bara måste kartläggas internt på myndigheten (enligt föreslagen brottsdataförordning 3 kap. 3 §) i stället för att redovisas öppet för berörda medborgare.

En anledning till att utredaren missat profileringsproblematiken kan misstänkas vara att profilering och därtill hörande dataskyddsproblem är näraliggande diskrimineringsproblematiken och därför kan ha förväxlats med densamma.[26] Diskriminering är emellertid något man utsätts för som specifik person i en specifik situation (man är en gravid kvinna med diabetes av ryskt ursprung som söker jobb, till exempel), medan skyddet mot profilering varken kräver att man besitter någon specifik, på förhand utsedd, minoritetsegenskap eller att man befinner sig i någon särskild situation.

Att inte införa bestämmelser som gör profilering förutsägbar och transparent i Brottsdatalag vore både att ignorera de skyldigheter som åligger svenska staten i och med godkännandet av EU:s nya dataskyddsdirektiv, men ur ett lokalt perspektiv skulle det också innebära att man förbiser de problem som redan påtalats av Integritetskommittén 2016.

Utredaren har valt att inte införa någon definition på ordet pseudonymisering, eftersom utredaren inte heller haft ambitionen att säkerställa bättre dataskydd vid diarieföring, arkivering och behandling av uppgifter och handlingar för historiska, statistiska eller forskningsrelaterade ändamål.

Pseudonymiseringen kommer dock till sin rätt vid sådana sammanhang, just därför att den kan tillåta bevarande av stora mängder handlingar och ärenden på ett offentligt och öppet sätt utan att för den delen ovillkorligen skapa ett dataskyddsintrång. En pseudonym i form av privatpersons initialer, eller i form

NJA PSEUDONYMISERAR

En praktisk och enkel analogi till pseudonymisering som skyddar en privatpersons integritet och samtidigt tillgodoser behovet av arkivering och forskning från den praktiserande förvaltningsjuristens vardag, är den pseudonymisering som sker i Nytt juridiskt arkiv och de prejudicerande beslut som tillgängliggörs på dom.se. Denna sorts pseudonymisering blir mindre explicit uppmuntrad av att utredaren inte föreslår göra det lätt för myndigheterna att redan från början arkivera sina handlingar enligt denna modell. Dataskyddet borde ses som ett kretslopp, där alla komponenter är viktiga.

[24] *Se t. ex.* Wikipedia https://sv.wikipedia.org/wiki/Sk%C3%A5nepolisens_register_%C3%B6ver_romer

[25] Mycket intressanta. Googla på *network analysis algorithm* eller *cluster algorithms*. Se även Engelin, M. och de Silva, F., Troll Detection – A comparative study in detecting troll farms on Twitter using cluster analysis, Kandidatuppsats i datavetenskap, KTH, 2016. Notera i avsnitt 3.2 att klusteralgoritmer är väldigt känsliga för *ingångsvärden* (utöver att de givetvis också påverkas av vilka uppgifter man låter dem behandla) vilket ökar behovet av transparens kring både val av algoritm och ingångsvärden när de används av myndigheter för att dra slutsatser om vilka åtgärder som behöver sättas in mot en eller flera enskilda.

[26] *Se t. ex.* Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion?, 6 januari 2016, USA:s regering *eller* Zuiderveen Borgesius, Frederik J., Online Price Discrimination and Data Protection Law (August 28, 2015).

av första bokstaven i förnamnet, ökar till exempel privatpersonens så kallade anonymitetskrets i förhållande till handlingen en hel del: eftersom fler personer har samma initialer än som har exakt samma egennamn, blir det svårare att återkoppla handlingen till någon specifik enskild (även om det så klart är möjligt med maskinella medel och kompletterande datamängder).

Dataskydd.net är av uppfattningen att ett införande av sådana enkla grepp, som på intet sätt kan antas störa myndigheternas möjligheter att vare sig diarieföra eller genomföra sina reguljära sysslor, på ett dramatiskt sätt kunde förbättra enskilda privatpersoners dataskydd och samtidigt garantera fortsatt insyn i de offentliga verksamheterna.

Utredaren har också valt att inte införa någon definition på ordet överföring, trots att utredaren själv observerar att det är oklart vad en överföring är och ska vara. Vi behandlar detta vidare i avsnittet om medborgares rättigheter i en globaliserad värld, s. 18.

Sammanfattning.

Avstyrker delvis: 6.2.

Begreppet *biometriska uppgifter* bör definieras som ”personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, och som möjliggör eller bekräftar unik identifiering av personen i fråga.”

Begreppet *profilering* bör definieras som ”behandling av personuppgifter som består i att dessa används för att bedöma personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga aspekter rörande dennas arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.”

Begreppet *pseudonymisering* bör definieras som ”behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.”

Begreppet *överföring* bör definieras som ”behandling av personuppgifter på ett sätt som innebär att uppgifterna skickas, vidarebefodras, förmedlas eller på annat sätt görs tillgängliga för någon i ett tredje land.”

Brottsdatalag 4 kap. 4 § ändras så att privatpersoner får en rätt att erhålla information om profilering även om profileringen inte har medfört något automatiserat beslut (utan till exempel ett manuellt beslut). Till exempel genom tilläget ”*Myndigheten ska också lämna information om profilering som genomförts eller genomförs mot den enskilde, eller mot kategorier av enskilda som den enskilde tillhör, även om sådan profilering bara har lett till manuella beslut.*”

Praktiska befogenheter, förpliktelser och tekniska lösningar (kapitel 8-10)

Personuppgiftsbiträdesrelationer mellan myndigheter eller mellan myndigheter och företag har för Dataskydd.net sett ut att uppstå i sådana situationer när en myndighet gör något bättre än en annan myndighet (till exempel handhar en viss databas eller ett visst IT-system),[27] eller då myndigheten som egentligen är personuppgiftsansvarig saknar erforderlig kompetens för att själva handha databasen eller IT-systemet.[28]

Därför är det underligt att utredaren föreslår att de skyldigheter som gäller systemdesign och databehandlingens tekniska förutsättningar att uppfylla dataskyddsprinciper bara ska åligga den personuppgiftsansvarige.[29] En personuppgiftsansvarig kommer inte att kunna vidta åtgärder för inbyggt integritetsskydd i ett datorsystem som inte står under den personuppgiftsansvarigas direkta kontroll. Själva poängen med att ha ett personuppgiftsbiträde försvinner också i hög utsträckning ifall den personuppgiftsansvariga måste besitta tillräcklig egen teknisk kompetens för att utvärdera personuppgiftsbiträdes lösningar i förhållande till de tekniska skyldigheter som åligger den ansvarige.

I den allmänna uppgiftsförordningen har man, med vetskap om att ovan beskrivna situation ofta även uppstår mellan privata företag, i stället infört en regel om att personuppgiftsbiträdet är skyldigt att bistå den personuppgiftsansvariga med sådana tips och råd som den senare kan behöva för att så effektivt som möjligt fullfölja sina skyldigheter enligt förordningen.[30] Man bör åtminstone ha en motsvarande bestämmelse i Brottsdatalag, även om den enklaste förändringen som går att göra i utredarens text är den vi föreslår.

Kontinuerligt kretslopp. Dataskydd är något som måste säkerställas genom att hela organisationen har en integrerad process för att åstadkomma dataskydd. Det behöver inkludera både leverantörer, beställare, organisatoriska omständigheter och verksamheten.

Bild: Genom recycling.com.

Den uteblivna definitionen av *pseudonymisering* gör att utredaren tvingas lägga förslag om både diarieföring och arkivering[31] som innebär ett större dataskyddsintrång än vad som vore fallet ifall pseudonymisering inte bara gavs en definition utan också infördes i lagtexten.

Lydelsen i 2 kap. 2 § bör ändras på sådant sätt att den kräver användning av pseudonymiserade uppgifter i så hög utsträckning som möjligt, till exempel genom att man i handlingarna inte använder egennamn eller samordningsnummer, utan initialer eller första bokstaven i förnamnet.

Med en sådan förändring i 2 kap. 2 § kommer det också att bli lättare att behandla handlingar för statistiska, historiska eller forskningsrelaterade ändamål[32] på ett sådant sätt att behandlingen uppfyller kraven på avidentifiering[33] i så hög utsträckning som möjligt.

God dataskyddspraktik behövs i hela värdekedjan för databehandling, vilket reflekterats i den europeiska lagstiftningen och därför bör föras in även i den

[27] *Se t. ex.* Prop. 2016/17:198, kap. 4.3 med förarbeten.
[28] *Ibid.*
[29] SOU 2017:29, kap. 10.6.5.
[30] Förordning 679/2016, art. 28.3.f.

> [*I*] *avtalet eller* [*r*]*ättsakten ska det särskilt föreskrivas att personuppgiftsbiträdet*
> */.../*
> *f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå*[.]

[31] SOU 2017:29, kap. 9.1.3.
[32] *Ibid.*, kap. 9.1.7.
[33] Förordning 679/2016, art. 89.1.

svenska implementationen. Den nyligen publicerade Digitaliseringsstrategin[34] bekräftar att regeringen är motiverad att säkerställa sig om god dataskyddspraktik i hela värdekedjan, och till och med sikta på att bli drivande på området.[35] Den ansträngningen börjar med att man inte gör lättsamma förbiseenden i Brottsdatalag.

Behandlingen av automatiserade beslut är så knapphändig[36] att Dataskydd.net bara delvis kan tillstyrka förslaget. Integritetskommitténs kartläggningar av polismyndighetens arbete med spaning på internet i delbetänkandet *Hur står det till med den personliga integriteten?*[37] indikerar snarare att det är just denna del i svensk dataskyddslagstiftning som kan vara i störst behov av utveckling.

Automatiserade beslut och *profilering* (ett begrepp utredaren har lämnat odefinierat, men som vi rekommenderar emot att man utelämnar från lagen) används i ökad utsträckning av brottsbekämpande myndigheter, särskilt vid automatiserade dataöverlämningar mellan olika länder. Frågan har varit föremål för prövning i EU-domstolen i samband med att EU-parlamentet lyfte avtalet om utbyte av passageraruppgifter i flygindustrin till granskning mot bakgrund av stadgan.

> 222. Av de uppgifter som har ingivits till domstolen framgår att överföringen av PNR-uppgifter som kan innehålla sådana känsliga uppgifter är fakultativ, det vill säga att de överförs endast när en passagerare beställt ytterligare service ombord. Det är emellertid uppenbart att en person som inte ännu har ”identifierats”, men som samarbetar med eller deltar i ett internationellt terroristnätverk eller nätverk för allvarlig brottslighet, av försiktighet kommer att undvika att använda sig av service som kan ge information om etniskt ursprung eller religiös övertygelse. De moderna utredningsmetoder som används av de behöriga kanadensiska myndigheterna och som, enligt vad som har förklarats för domstolen, består i att dessa myndigheter korsjämför de erhållna PNR-uppgifterna, vilka kan grunda sig på känsliga uppgifter eftersom detta inte är förbjudet enligt det planerade avtalet, med scenarier eller typprofiler för personer som innebär en risk, möjliggör slutligen endast behandling av känsliga uppgifter om personer som legitimt har beställt ytterligare service ombord och mot vilka det inte finns och sannolikt inte kommer att finnas några misstankar. *Den risk för stigmatisering av ett stort antal enskilda, vilka dock inte är misstänkta för något brott, som användningen av dessa känsliga uppgifter innebär framstår som särskilt oroande och jag föreslår därför att domstolen ska slå fast att dessa uppgifter ska uteslutas från det planerade avtalets tillämpningsområde.*
>
> – Generaladvokat Paolo Mengozzi i Yttrande 1/15.[38] [vår kursivering]

I utredningen om en ny utlänningsdatalag beskrivs utförligt hur nya teknologier, som automatiska bildigenkänningssystem och korskörning av fingeravtrycksregister, ska användas för att utifrån biometriska uppgifter kunna dra slutsatser om vilka typer av inresande som ska utsättas för starkare granskning.[39] Utredningen beskriver även andra typer av informationsdelning som hjälper myndigheterna att bygga typprofiler som stöd för deras brottsutredande verksamhet.

---

[34] Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D).
[35] *Ibid.*, s. 18–19.
[36] SOU 2017:29, kap. 9.4.
[37] SOU 2016:41, s. 500 (kapitel 18.7.3).
[38] ECLI:EU:C:2016:656, Yttrande 1/15, punkt 222, föredraget 8 september 2016.
[39] SOU 2015:73, kap. 7.10.

Exemplena ovan beskriver *automatiska beslut* så till vida att man på grund av uppgifter man samlar in inleder närmare granskningar och utredningar av dessa personer, men det är inte ett *beslut* i den mening som avses i svensk lag med begreppet *myndighetsbeslut*. EU-lagstiftningen använder begreppet *profilering* för att komplettera lagstiftning som tidigare inte tog i beaktande dessa sorters automatiska beslut.

Den innevarande utredaren påtalar till och med själv i sin genomgång av *kontrollverksamhet* att kontrollerade individer bör upplysas om iakttagelser som gjorts vid en kontroll och om de handlingar eller föremål som säkrats till grund för förundersökningar.[40] Till sådana handlingar bör alltså, enligt Dataskydd.net, räknas information om profileringsåtgärder och beteendekartläggning, men vi ser inte att utredarens förslag ger förutsättning för den sortens transparens. Trots att den alltså egentligen är explicit stadgad i EU-direktivet.

Behandlingen av utredningens kapitel 10.4 lämnas till s. 19.

Sammanfattning.

Tillstyrker: 9.1.1, 9.1.2, 9.1.5, 9.1.6, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.2, 9.5, 9.6, 10.1.1, 10.1.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.2.8, 10.3, 10.5.1, 10.5.2, 10.5.3, 10.6.1, 10.6.2, 10.6.3, 10.6.4, 10.7.2.

Avstyrker delvis: 9.1.3, 9.1.7, 9.4, 10.6.5.

Avstyrker: 10.8

Brottsdatalag 2 kap. 2 § kompletteras med stycket ”Uppgifterna ska pseudonymiseras om inte detta vore uppenbarligen orimligt eller förhindra vidare handläggning av ärendet.”

Brottsdatalag 2 kap. 5 § kompletteras med stycket ”Uppgifterna ska pseudonymiseras om det inte finns särskilda skäl till varför detta vore olämpligt.”

Brottsdatalag 3 kap. 20 § ändras till lydelsen ”Det som sägs om den personuppgiftsansvariges skyldigheter i 3, 5, 6, 8 och 12 §§ gäller även för personuppgiftsbiträden.”

Brottsdatalag 4 kap. 4 § ändras så att privatpersoner får en rätt att erhålla information om profilering även om profileringen inte har medfört något automatiserat beslut (utan till exempel ett manuellt beslut). Till exempel genom tilläget ”*Myndigheten ska också lämna information om profilering som genomförts eller genomförs mot den enskilde, eller mot kategorier av enskilda som den enskilde tillhör, även om sådan profilering bara har lett till manuella beslut och även då sådan profilering använts inom ramen för kontrollverksamhet som senare lett till brottsutredning.*” Se vidare s. 4.

Effektiv tillsyn? (kapitel 12)

Dataskydd.net välkomnar förslaget att tillsynsmyndigheten ska ges uppdraget att å enskilda privatpersoners vägnar kontrollera att uppgifter behandlas

[40] SOU 2017:29, s. 199 (kap. 8.2.10).

författningsenligt.[41]

Dataskydd.net instämmer också med utredningens observation att de statliga utredningarna kring tillsyn av den personliga integriteten skapar ett komplicerat nätverk av olika grupper som på olika sätt och utifrån olika förutsättningar bedömer tillsynsfrågorna.[42] Utredningen om tillsyn av den personliga integriteten[43] fann sig till exempel nödgad att observera att den inte hade tillräckligt med insyn och förståelse för de parallellt pågående utredningarna om införlivandet av dataskyddsförordningen och dataskyddsdirektivet i svensk rätt för att kunna bedöma vilken sorts tillsyn som eventuellt kunde behövas.[44] I Stället är det utredningen om en ny dataskyddslag som har tagit ledartröjan i att definiera vad Datainspektionens uppgifter ska vara under den nya lagstiftningen.[45] Det här komplicerar läget även för de som försöker följa de statliga dataskyddsutredningarna, och för de som så småningom kommer behöva följa dataskyddslagarna.

Vi ifrågasätter starkt behovet av att lagstadga en förpliktelse för Datainspektionen att bara genomföra tillsynsåtgärder i en plågsam och långdragen sexstegsraket bestående av förhandssamråd, råd, rekommendationer, påpekanden, varningar och först därefter riktiga förelägganden och beslut.

Tillsynsmyndigheten föreslås redan förpliktigas att ge råd och stöd vid förhandssamråd och när det i övrigt är påkallat (Brottsdatalag 5 kap. 4§). Enbart utifrån denna bestämmelse borde behovet av ytterligare en lagstadgad förpliktelse att ge råd och rekommendationer kunna antas vara lågt. Om de tillsedda myndigheterna inte till att börja med velat eller gitt lyssna på råd och rekommendationer kan det inte antas att de kommer motiveras av att höra samma råd och rekommendationer två gånger.

Påpekanden och förutsättanden har varit Datainspektionens huvudsakliga arbetsmetod fram till idag. Resultaten av dessa åtgärder är nedslående. Tillsedda myndigheter tar flera år på sig att åtgärda felaktigheter om de alls gör det.[46] Dessutom är utvecklingen av praxis på dataskyddsområdet är i princip obefintlig[47] till följd av att Datainspektionen sällan kommer till skotts (utredningen om en ny dataskyddslag anmärker att Datainspektionen aldrig använt vitesinstrumentet i personuppgiftslagen[48]). Utredaren observerar själv att tillsedda brottsbekämpande myndigheter är saktfärdiga eller ovilliga att rätta sig efter

Inte något vilddjur. Tillsynsmyndigheten för dataskydd behöver inte tyglas på sådant sätt att den bara efter mycket långdragna administrativa processer får ägna sig åt den egentliga tillsynen. Tvärtom riskerar allt för stora hinder för förelägganden och beslut att leda till utdragen juridisk osäkerhet och oförmåga för tillsynsmyndigheten att upprätthålla och tillse lagen på ett tillfredsställande vis.

Bild: Fenrisulven i strid med två vikingar så som avbildad i det isländska 1700-talsmanuskriptet NKS 1867 4TO som idag finns på Det Kongelige Bibliotek i Danmark.

[41] *Ibid*., kap. 12.6.3.
[42] *Ibid*., s. 430
[43] SOU 2016:65
[44] *Ibid*., s.
[45] SOU 2017:39, s.
[46] *Jfr*. Datainspektionens Dnr 1546-2016 om tillsyn enligt personuppgiftslagen (1998:204) – behörighetstilldelning, spärrar m.m enligt patientdatalagen riktad mot Hälso- och sjukvårdsnämnden i Region Gävlebord.
[47] SOU 2016:41, s. 630:

> *Domstolsverket kan inte ta fram statistik som visar hur många mål om ersättning i form av skadestånd enligt personuppgiftslagen som prövas i svenska tingsrätter. Kommittén har genom sökning på Infotorg endast fått fram en handfull domar. Vår sökning visar att landets tingsrätter endast avgjort fem sådana mål under perioden 2012–2015. Två av dessa ogillades utan att stämning väcktes. De tre andra prövades i sak. I två av dessa ogillades käromålet. I det tredje fick käranden en liten del av sin talan bifallen.*
>
> *Domstolsverket kan inte heller ta fram statistik över mål där yrkanden har prövats om ersättning för kränkning av den personliga integriteten med stöd av 2 kap. 3 § skadeståndslagen i landets tingsrätter. Det är enligt Domstolsverket mycket osannolikt att fråga om kränkningsersättning prövats som separat mål.*

[48] SOU 2017:39, s. 297.

rekommendationer och påpekningar från Datainspektionen och Säkerhets- och integritetsnämnden.[49] För att undvika sådana situationer som uppstått kring datalagring,[50] Safe Harbor-beslutet,[51] och bloggande om kollegors hälsotillstånd[52] bör man snarare uppmuntra Datainspektionen att snabbare komma till beslut och, vid behov, inleda en rättslig prövning. Den juridiska osäkerheten kring flera av direktivets och den svenska lagstiftningens paragrafer kommer ändå, mot bakgrund av att de alla är underställda EU-stadgans artikel 7 och 8, att vara påtaglig under lång tid. Men tidsperioden kan förkortas av att Datainspektionen får göra sitt jobb i stället för råda, stöda, råda, rekommendera, påpeka och varna (i den ordningen).

Vi ser heller inga skäl att frånta Datainspektionen möjligheten att förena förelägganden med viten. Snarare ser vi att Datainspektionens nuvarande oförmåga att för det första alls utfärda förelägganden, och för det andra förena dessa med viten, leder till att åtgärder mot överträdelser försenas eller helt uteblir.[53] Detta har även observerats av Integritetskommittén.[54] Snarare kan vitesföreläggande vara ytterligare ett sätt att snabbare få till stånd de rättsliga prövningar som behövs för att klargöra medborgarnas rättigheter och myndigheternas skyldigheter. Vi återvänder till sanktioner och viten i nästkommande avsnitt.

De myndigheter som täcks av Brottsdatalag och tillhörande förordning måste antas vara tillräckligt kompetenta för att i första hand förmå sig själva följa lagstiftningen, utan att Datainspektionen daltar med det. Tillsynsmyndigheten kan antas kunna hålla sig sysselsatt utan att åläggas att handskas med dessa kompetenta myndigheter med silkesvantar.

Det är förvånande att utredaren verkar definiera tillsynsmyndighetens oberoende utifrån medborgaren, och inte utifrån regeringen.[55] Tillsynsmyndigheters oberoende har redan behandlats av EU-domstolen i ett antal uppmärksammade fall och har där rört myndigheternas oberoende av den politiska makten.[56] Även om den svenska tillsynstraditionen innebär att tillsynsmyndigheterna ska agera för att upprätthålla lagen i *det allmännas* intresse,[57] är det uppenbart att den europeiska lagstiftningen nu drar tillsynen av dataskydd i den riktning att den ska bedrivas i *allmänhetens* intresse.[58]

[49] SOU 2017:29, s. 427.

[50] ECLI:EU:C:2017:222, C-203/15.

[51] ECLI:EU:C:2015:650, C-362/14.

[52] ECLI:EU:C:2003:596, C-101/01.

[53] Se ovan fotnot 46.

[54] SOU 2016:41, s. 619–620.

[55] SOU 2017:29, s. 431, 442.

[56] *Se t. ex.* ur ECLI:EU:C:2010:125, C-518/07:

> *36. Det ska dessutom understrykas att risken att kontrollmyndigheterna kan påverka tillsynsmyndigheternas beslut i politiskt hänseende i sig är tillräcklig för att hindra tillsynsmyndigheterna från att utöva sina uppgifter oberoende. För det första kan dessa myndigheter, såsom kommissionen har påpekat, visa en ”föregripande hörsamhet” med hänsyn till kontrollmyndighetens beslutspraxis. För det andra förutsätter den roll som väktare av rätten till privatliv som nämnda myndigheter har, att deras beslut, och följaktligen de själva, är höjda över varje misstanke om partiskhet.*

Men också exempelvis ECLI:EU:C:2012:631, C-614/10, och ECLI:EU:C:2014:237, C-288/12.

[57] *Jfr.* regeringens skrivelse 2009/10:79, kap. 3.2:

> [*Tillsyn*] *avser självständig granskning för att kontrollera om tillsynsobjekt uppfyller krav som följer av lagar och andra bindande föreskrifter och vid behov kan leda till beslut om åtgärder som syftar till att åstadkomma rättelse av den objektsansvarige.*

[58] Vilket Skrv. 2009/10:79 också godtar (”*Medborgarna ska genom tillsynen vara förvissade om att deras intressen tas till vara.*”), bara inte i någon definition.

Handlingsimperativet bakom den europeiska lagstiftningen är alltså att *det allmänna* är en sorts dataskyddsantagonist gentemot *allmänheten*,[59] och att tillsynsuppdraget ska reflektera den omständighet att även offentliga verksamheter och organ kan kränka individuella rättigheter.[60]

Om tillsynen i enlighet med logiken bakom dataskyddsdirektivets tillsynsbestämmelser ska utformas så att den på bästa sätt tillvaratar allmänhetens intressen, i stället för det allmännas intressen, behöver justeringar göras i utredarens bedömning av hur klagomål från enskilda ska hanteras, vilken relation enskilda ska ha till beslut fattade av tillsynsmyndigheten, samt förutsättningarna för enskilda att få råd och rekommendationer från tillsynsmyndigheten.

Enskilda medborgare som grunnar på sina rättigheter kan vara i lika stort behov av råd och rekommendationer från tillsynsmyndigheten som personuppgiftsansvariga och personuppgiftsbiträden är. Det kan till exempel röra frågor om den svenska lagstiftningens relationer till den europeiska stadgan,[61] lagstiftningens förhållande till eller tolkning mot bakgrund av grundlagen eller tillämpningsområdet för den svenska lagstiftningen.

Eftersom tillsynsmyndigheten precis som de tillsedda myndigheterna tillhör det allmänna och det allmännas intressesfär är det olyckligt att enskilda inte kan överklaga tillsynsbeslut.[62] Målsättningen med den europeiska lagstiftningen är att enskilda ska ges ett effektivt skydd för sina fri- och rättigheter, till vilket räknas effektiva möjligheter att själv utöva rättigheterna. Den svenska tillsynspraxis för dataskydd som beskrivs av utredaren innebär i stället att den enskilde förpassas till en passiv, mottagande roll av sin rätt till privatliv och dataskydd.

Utredningen verkar har missförstått direktivets artikel 46.3 som anger att tillsyn ska vara avgiftsfri för registrerade och för dataskyddsombud.[63] Det innebär en omvänd situation från den som utredaren framhåller, eftersom utredaren

[59] Se även ECLI:EU:C:2010:125, C-518/07.

[60] I SOU 2015:39 Myndighetsdatalag föreslogs en presumtion att myndigheter inte kan kränka integriteten, som Dataskydd.net givetvis bemötte i sitt remissyttrande över förslaget. Även om utredaren i Brottsdatalag inte har försökt återuppliva en sådan missriktad presumtion, är blotta förekomsten av en sådan tankebana i en statlig utredning år 2015 en indikation på att det svenska förvaltningsväsendet och dess politiska huvudmän på departementen inte nödvändigtvis införlivat de kontinentaleuropeiska resonemangen kring förhållandet mellan medborgare och stat som präglar EU:s dataskyddslagstiftning.

[61] Under 2016 försökte Dataskydd.net ta reda på om bestämmelserna för registerutdrag i PUL 26 §mot bakgrund av att registerutdrag är en rättighet enligt Art. 8, EU:s stadga för grundläggande rättigheter också var tillämplig på sådana uppgifter som lagrats enligt LEK 16a §. Datainspektionen undvek att svara på frågan genom att hänvisa till en då ännu inte avslutad prövning i EU-domstolen av polisens möjligheter att begära sådana uppgifter utlämnade. Frågan förefaller vara sådan att Datainspektionen enkelt borde ha kunnat besvara den utifrån deras kunskap om EU-rättens ställning i förhållande till svensk rätt, det faktum att både PUL och LEK-bestämmelserna härrörde från EU-rätten och EU-stadgans tillämpning på sådan lagstiftning som ligger inom EU:s lagstiftningskompetens. Att Datainspektionen undvek att svara på frågan innebar att den privatperson som Dataskydd.net vid tillfället samarbetade med fick mycket sämre möjligheter att hävda sin rätt gentemot en svensk teleoperatör, som med hänvisning till Datainspektionens uteblivna precisering av rättsläget inte ville lämna ut uppgifterna. Eftersom Datainspektionen vägrade ge något definitivt svar med hänvisning till att de eventuellt kunde komma att besvara frågan vid ett senare tillfälle hade privatpersonen heller ingen möjlighet att överklaga Datainspektionens tolkning.

[62] SOU 2017:29, s. 448.

[63] Direktiv No. 680/2016, art. 46.3:

> *Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och för dataskyddsombudet.*

tycker att Datainspektionen ska kunna ta betalt för dataskyddsombudsutbildningar och för information till allmänheten som Datainspektionen producerar, men inte för tillsynsåtgärder.[64] Med den ordning som utredaren föreslår riskerar kunskapen om och bristen på information kring Brottsdatalag mening och tolkning bli svårtillgänglig på ett för alla oönskat vis.

Eftersom inspektionens funktion att tillgodose behovet av förhandssamråd och tolkningsfrågor kring den nya lagstiftningen kan antas vara stort, är det rimligt att inspektionen kan ta ut obligatoriska administrativa avgifter av tillsynsobjekt på samma sätt som till exempel Post- och telestyrelsen tar ut administrativa avgifter av licensförpliktigade leverantörer av allmänna elektroniska kommunikationnät.[65] Departementet kan i detta notera att dataskyddsombudet som ska utses vid personuppgiftsansvariga myndigheter och hos personuppgiftsbiträden inte ersätter tillsynsverksamhet mot dessa, utan bara ska utgöra en rådgivande stödfunktion inom organisationerna.[66]

Om Datainspektionen fortsatt ska finansieras med 100 % statliga anslag finns en risk att den underfinansierade Datainspektionen inte kommer att kunna ge råd, samråd, rekommendationer, påpekanden och varningar som är tillräckligt adekvata i förhållande till lagstiftningen. Inspektionens funktion som stöd till både allmänheten och dataskyddsombuden riskerar då att bli bristfällig.

Det är också tveksamt ifall inspektionen kommer att kunna bistå i tolkningsfrågor, till exempel när det uppstår tveksamheter kring hur rättspraxis från EU-domstolen eller Europadomstolen påverkar tillämpningen av svensk lag i Sverige (vilket de ju kan göra och vid ett antal tillfällen har gjort).[67]

Sammanfattning.

Tillstyrker: 12.4.1, 12.4.2, 12.5.2, 12.6.3, 12.7.3, 12.8.2, 12.8.4, 12.10.1, 12.10.2

Avstyrker delvis: 12.6.1, 12.6.4, 12.7.5, 12.7.6, 12.9, 12.11.1, 12.11.2

Avstyrker: 12.6.2.

Brottsdatalag 5 kap. 6 § kan tas bort. Uppgifterna i 5 kap. 6 § täcks redan av texten i 5 kap. 4 §.

Brottsdatalag 5 kap. 7 § 1 stycket punkt 1 kan tas bort. Uppgifterna i 5 kap. 6 § täcks redan av texten i 5 kap. 4 §.

Brottsdatalag 5 kap. 7 § 2 stycket kompletteras med texten ”Föreläggan-den kan förenas med vite.”

[64] SOU 2017:29, s. 483.

Enligt 3 och 4 §§ avgiftsförordningen (1992:191) får en myndighet ta ut avgifter för varor och tjänster som den tillhandahåller endast om det följer av lag eller förordning eller av ett särskilt beslut av regeringen. Därutöver får en myndighet ta ut avgift i vissa fall, bl.a. för att tillhandahålla information, rådgivning och annan service, om det är förenligt med myndighetens arbetsuppgifter enligt lag, in- struktion eller annan förordning och verksamheten är av tillfällig natur eller av mindre omfattning. Enligt 2017 års regleringsbrev får Datainspektionen ta ut avgift för varor och tjänster även om de inte är av tillfällig natur eller mindre omfattning. Det som avses är rät- ten för myndigheten att ta ut ersättning för den omfattande utbildningsverksamhet som den bedriver.

[65] Post- och telestyrelsen, Årsredovisning 2016 (PTS-ER-2017:01), s. 59.

[66] Direktiv No. 680/2016, art. 32–34.

[67] *Jfr*. ECLI:EU:C:2015:639, C-230/14 eller EDMR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (Application no. 931/13).

Det bör förtydligas att rätten till överklagande som anges i 7 kap. 4 § också gäller privatpersoner som drabbas av tillsynsmyndighetens beslut.

Implikationerna av att ändra premisserna bakom Brottsdataförordning 5 kap. 10 § går bortom vad vi kan täcka i det här remissyttrandet.

Sanktioner, viten och rättsmedel (kapitel 13-14)

Dataskydd.net välkomnar förslaget om införandet av en ny administrativ sanktionsavgift,[68] och stödjer förslaget om att inte införa någon ny straffbestämmelse.[69] Vi välkomnar också att både personuppgiftsansvariga och personuppgiftsbiträden kan åläggas administrativa sanktionsavgifter[70] och anser, i likhet med utredaren, att det är tillsynsmyndigheten som ska besluta om sanktionsavgifter.[71] Vi är också överens om att ansvaret ska vara strikt.[72]

Vi ser också de föreslagna reglerna om dröjsmålstalan som ett sätt att stärka privatpersoners möjligheter att utöva sina rättigheter genom tillsynsmyndigheten.[73] I verksamheter som kräver större sekretess, och det är sådana verksamheter som kommer täckas av Brottsdatalag, blir det extra viktigt för privatpersoner att kunna förlita sig på att det går att få Datainspektionen att agera i deras ställa. Vi välkomnar därför också möjligheten att genom Datainspektionen begära en kontroll av lagligheten i en viss personuppgiftsbehandling.[74]

Vi är kritiska mot att utredaren inte anser att vägran att samarbeta med tillsynsmyndigheten ska kunna sanktioneras.[75] Eftersom tillsynsmyndigheten kommer att vara i stort behov av samarbete från de tillsedda verksamheterna att få sådan information de behöver för att göra en bedömning av dataskyddet på de tillsedda verksamheterna ser det ut som en allvarlig överseelse.

Vi är också kritiska mot att utredaren inte anser att en verksamhet ska kunna sanktioneras om den struntar i att uppfylla sina förpliktelser mot enskilda privatpersoner.[76] Det förefaller annars vara poängen med direktivet att just stärka och förbättra enskildas dataskydd.

Det är i vår mening inte klokt att inte möjliggöra sanktioner för de tillfällen då en verksamhet slarvat med personuppgiftsbiträdesavtal. Eftersom dessa avtal i hög utsträckning kommer att definiera vilken sorts rättigheter privatpersoner får gentemot tredje parter - sådana parter som behandlar privatpersonernas uppgifter å den personuppgiftsansvariges vägnar - känns det i alla fall rättsligt relevant att det någonstans finns ett avtal som går att granska. I kombination med att utredaren föreslår göra det riskfritt[77] att inte samarbeta med tillsynsmyndigheten kan det här få allvarliga konsekvenser för privatpersoners möjligheter att utöva sin rätt till dataskydd.

Vi är besvikna över att utredaren frångår de sanktionsnivåer som fastställs

[68] SOU 2017:29, kap. 13.2.2.
[69] *Ibid.*, kap. 13.2.1.
[70] *Ibid.*, kap. 13.4.
[71] *Ibid.*, kap. 13.7.1.
[72] *Ibid.*, kap. 13.5.3.
[73] *Ibid.*, kap. 14.6.2 och 14.6.3.
[74] *Ibid.*, kap. 12.6.3.
[75] *Ibid.*, kap. 10.2.6 och kap. 13.5.2, i kombination med Brottsdatalag 6 kap. 1 §.
[76] *Ibid.*, s. 509.
[77] Se ovan fotnot 75.

i den allmänna dataskyddsförordningen.[78] Eftersom de administrativa sanktionerna ska utdömas mot bakgrund av vad som är rimligt och lämpligt, finns det inget skäl att tro att tillsynsmyndigheter kommer att utdöma den maximala möjliga administrativa sanktionsavgiften annat än om något extremt exceptionellt har inträffat. Sanktionerna behöver däremot vara på en sådan nivå att de motsvarar obehaget och kostnaden av att förändra organisatoriska och tekniska rutiner hos de myndigheter som träffats av ett beslut om administrativa sanktioner, och de föreslagna sanktionerna uppgår inte nödvändigtvis till sådana nivåer. Det handlar alltså inte om att sanktionsstorleken skulle vara något mått på den ondska man tror finns på den som drabbas av tillsynen,[79] utan om hur sanktionerna kan bidra till att den tillsedda aktören får ekonomiska incitament att agera på tillsynens resultat.

¿ €€€?
Hur stora sanktioner?

De administrativa sanktionerna bör vara i den maximala storleksordningen att de motsvarar myndigheternas ungefärliga kostnader för att ändra på IT-system och organisatoriska rutiner kring datahantering. Att rätta till dataskyddsproblem måste helt enkelt löna sig, även i en ekonomisk effektivitetskalkyl. Det gör det bara om det är dyrare att göra fel än att göra rätt.

Utredaren föreslår att Datainspektionen inte ska kunna förena sina förelägganden med viten.[80] Viten är emellertid ett bra sätt att se till att det kostar mer att inte göra som Datainspektionen förelägger, än att strunta i att göra som Datainspektionen förelägger. Viten kan, utifrån ett säkerhetsekonomiskt perspektiv, antas fungera extra bra när en personuppgiftsansvarig eller personuppgiftsbiträde gjort så stora brister i grundarbetet kring en viss databehandling att kostnaden för att ändra på rutiner och tekniska system är stor.

Integritetskommittén har observerat att Datainspektionens tillsyn har blivit mindre effektiv av att de inte kan förena förelägganden med viten.

> Datainspektionen har i en skrivelse till Regeringen i december 2011 framfört att det finns behov av att på ett allmänt plan se över myndighetens roll och uppdrag. En brist som Datainspektionen särskilt uppmärksammade var begränsningen i möjligheten att förena sina förelägganden och förbud med vite, särskilt i samband med tillsyn inom hälso- och sjukvården.
>
> — Integritetskommittén, SOU 2016:41.[81]

För den sortens förelägganden som Datainspektionen kan tänkas utfärda under Brottsdatalag gäller särskilt att en frånvaro av möjligheter att förena förelägganden med viten riskerar att leda till långvariga överträdelser. Datainspektionen måste genomgå hela fem steg av samråd, råd, förklaranden, påpekanden, och varningar innan de kommer fram till den punkt då de kan besluta att en myndighet gjort något fel som ska rättas till. Sedan måste Datainspektionen sannolikt repetera samma övning igen för att kunna utdöma den administrativa sanktionsavgiften.

Resultatet blir ett dåligt skydd för medborgare och en till synes obegripligt handlingsförlamad Datainspektion. Det vill säga motsatsen till det som den europeiska lagstiftaren föreskrivit ska gälla för en dataskyddsmyndighet.

Utredaren har inte gjort någon ansats att åtgärda privatpersoners möjligheter att oberoende av tillsynsmyndigheten utöva sin rätt till dataskydd.[82] Integritets-

[78] SOU 2017:29, kap. 13.6.1.

[79] Utredaren skriver på s. 513 i SOU 2017:29 att ”*felaktigt handlande av en myndighet sällan föranleds av en önskan att maximera vinst eller att göra en större besparing, även om det inte kan uteslutas att det finns ekonomiska motiv*.” Detta överensstämmer inte med de rapporter i medier som förekommer om felaktiga IT-investeringar, senast i somras Transportsstyrelsens överlåtande av sin IT-infrastruktur på IBM (som ledde till att GD blev bötfälld för vårdslös hantering av sekretessklassad information).

[80] SOU 2017:29, s. 473

[81] SOU 2016:41, s. 620.

[82] *Ibid.*, kap. 14.3 och 14.4.

kommittén observerade under 2016 att skadeståndsnivåerna vid dataskyddsöverträdelser är på en sådan nivå att de inte rimligen kan antas vara en möjlig väg framåt för privatpersoner att utöva sin rätt.[83]

Domstolarna behöva frångå den föreställning som Integritetskommittén observerat att skadestånd inte har en normerande verkan.[84] Det kommer i sin tur bara att ske genom att rättskällorna (så som statliga utredningar) erkänner att detta är en felaktig föreställning. Utredaren ger sorgligt nog snarare intrycket av att ha helt ignorerat påtalanden om att skadeståndsbestämmelserna hittills inte fungerat, genom att särskilt ange att myndigheter inte ska antas göra fel av ekonomiska skäl.[85]

Vi är också kritiska mot att utredningen inte gjort någon ansats att förenkla grupptalan.[86] Utredaren har i stället tolkat ideella föreningars möjligheter att representera enskilda privatpersoner som ombud, men detta är felaktigt. Eftersom personuppgifter från många olika privatpersoner ofta behandlas samtidigt, kan det till exempel hända att en överträdelse av dataskyddsregler drabbar många personer samtidigt. Detta kan vara fallet om en brottsbekämpande myndigheter inte delger privatpersoner information om en säkerhetsincident de drabbats negativt av, eller om de brottsbekämpande myndigheterna upprättar olagliga register eller överför uppgifter eller på annat sätt tillskansar sig uppgifter på ett regelvidrigt sätt.

Målsättningen som har funnits i vissa medlemsländer, till exempel Frankrike,[87] har varit att få en sådan situation att ideella föreningar kan representera enskilda privatpersoner i dataskyddsfrågor på samma sätt som en svensk organisation för kollektiv upphovsrättsförvaltning kan representera konstnärer. Utan privatpersonens föregående uttryckliga samtycke, men ändå med mandat att processa i domstol å dennes vägnar. Det är ett sätt för registrerade att få kollektiv makt och kollektiva möjligheter att utöva sina rättigheter även när det vore väldigt svårt för de registrerade att ensamma göra detta. I dataskyddsfrågor kan detta vara extra lämpligt, eftersom både de tekniska infrastrukturerna som används av myndigheterna vid uppgiftsbehandling är komplicerade och kräver specialkunskap för att analysera och de juridiska regelverken som kringgärdar de tekniska systemen är likaledes komplicerade och kräver specialkunskap.[88]

Grundfrågeställningen är alltså egentligen hur man ska göra det (ekono-

[83] SOU 2016:41, s. 636–637. Se särskilt kap. 3.3.6 ur samma utredning:

Generellt för hela området är att sanktionssystemet, både det straffrättsliga och det skadeståndsrättsliga, inte verkar användas i någon större omfattning. Det är i alla fall mycket få ärenden som når domstolarna. Exempelvis har vi för perioden 2012–2015 endast funnit fem tvistemål i tingsrätt där frågan handlat om skadestånd enligt personuppgiftslagen (1998:204). Det ser inte annorlunda ut på straffrättens område. Under år 2014 avgjordes sammanlagt i landet endast fyra ärenden om brott mot personuppgiftslagen (genom domslut, strafföreläggande eller åtalsunderlåtelse).

När systemet väl används rör det sig om lindriga straff och låga skadeståndsbelopp. Sammanfattningsvis kan sanktionssystemet inte sägas fungera fullt ut, eftersom det inte har fått den effekt som avsågs med bestämmelserna.

[84] Se SOU 2016:41, s. 622: ”*I förarbeten till skadeståndslagen tonades dock den preventiva funktionen ner. Det anfördes att skadeståndsreglernas moralbildande och preventiva funktion var överdriven.*”

[85] Se ovan fotnot 79.

[86] SOU 2017:29, kap. 14.9.

[87] *Se t. ex.* UFC-Que Choisir (9 juni 2014) ”*Action de groupe – Du nouveau!*”

[88] *Jfr.* i detta avseende också Laurie Cranors studier om konsumentavtal för digitala tjänster. Vi hänvisar till källförteckningen längre ned.

miskt) rationellt för enskilda privatpersoner att hävda sin rätt.

Sammanfattning.

Tillstyrker: 13.2.1, 13.2.2, 13.4, 13.5.3, 13.6.2, 13.7.1, 14.6.2, 14.6.3, 14.7.1.

Avstyrker delvis: 13.5.2, 13.7.2, 13.7.3, 14.3.2.

Avstyrker: 13.6.1, 14.5, 14.9.

Brottsdatalag 6 kap. 1 § 1 stycket kompletteras med punkten ”4. 4 kap. 1-4 §§ samt 9-10 §§.”

Brottsdatalag 6 kap 1 § 1 stycket punkt 2 kompletteras med ”3 kap. 12 §” och ”3 kap. 17-18 §§”.

Brottsdatalag 6 kap. 3 § 1 stycket ändras så att anvisningen till högsta-beloppet för sanktionsavgiften sätts till 1 % av myndighetens eller verksamhetens årsomsättning.

Brottsdatalag 6 kap. 3 § 2 stycket ändras så att anvisningen till högsta-beloppet för sanktionsavgiften sätts till 2 % av myndighetens eller verksamhetens årsomsättning.

Rättssäkerhet för privatpersoner i en globaliserad värld (kapitel 15)

Vi är inte eniga med utredarens bedömning att det inte behövs en definition av ordet överföring. Dels menar vi att omständigheten att utredaren känt ett behov av att klargöra vad den menar med en överföring talar emot att det saknas ett behov av att definiera begreppet. Dels ser vi att utredaren själv påtalat att det finns oklarheter kring vad den överföring ska vara, till exempel om man ”befinn[er] sig i ett tredjeland och där ha[r] elektronisk tillgång till personuppgifter som [lagras på en server] i hemlandet.”[89]

Det är för Dataskydd.net ganska klart, och verkar vara så även för utredaren,[90] att även den omständigheten att man ges åtkomst till personuppgifter som är lagrade i ett svenskt IT-system och inte själv befinner sig i Sverige bör ses som en överföring. I syfte att klargöra det juridiska läget bör det skrivas in en definition i ramlagen. Detta gäller inte minst för att få tydlighet kring villkoren som gäller för outsourcing av drift och underhåll av IT-system.

Utredarens förslag lämnar också något att önska i sin behandling av beslut om adekvat skydd. Dels kan EU-kommissionens beslut om adekvat personuppgiftsskydd i tredje land inte alltid anses tillförlitliga. Detta har vi erfarit i och med *Schrems*-målet hösten 2015.[91] Dels måste Datainspektionen, enligt samma domslut, ha möjligheter att genomföra tillräcklig och fullgod tillsyn av dataskyddet i det tredje landet enligt EU-domstolens beslut i första datalagringsmålet.[92]

De föreslagna reglerna kan inte anses uppfylla detta krav.

Problemet med att redan från början inte ta höjd för att EU-kommissionen i stället för att uppfylla sina stadgeenliga förpliktelser att skydda europeiska

[89] SOU 2017:29, s. 573.
[90] *Ibid.*, s. 573–574.
[91] ECLI:EU:C:2015:650, C-362/14.
[92] ECLI:EU:C:2014:238, C-293/12.

medborgares rättigheter lägger sig för politiska påtryckningar från medlemsländerna och godtar ett svagare skydd för dataskyddet i ett tredje land än vad som objektivt sätt krävs utifrån EU:s stadga och EU-domstolens praxis, är att EU-domstolen då, när EU-domstolen gör det EU-domstolen måste göra och upprätthåller de europeiska medborgarnas rättigheter, kan komma att skapa stora problem för de brottsbekämpande myndigheternas verksamhet. Departementet bör vilja undvika den situationen, och kan också undvika den situationen genom att inte tvinga EU-domstolen att i efterhand underkänna departementets ansträngningar.

Sammanfattning.

Tillstyrker: 15.2.2, 15.2.3, 15.2.4, 15.2.5, 15.3.1, 15.3.2, 15.3.4, 15.5, 15.6.1, 15.6.2, 15.6.4, 15.6.5, 15.6.6, 15.7, 15.8.1, 15.8.2, 15.8.3,15.10.

Avstyrker delvis: 15.2.1, 15.6.3, 15.6.7, 15.8.4.

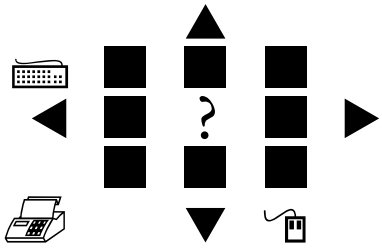
Avstyrker: 15.3.3, 15.4, 15.9.1.

Begreppet *överföring* bör definieras som ”behandling av personuppgifter på ett sätt som innebär att uppgifterna skickas, vidarebefodras, förmedlas eller på annat sätt görs tillgängliga för någon i ett tredje land.”

Insyn är den enskildes bästa verktyg för ansvarsutkrävande (kapitel 10-11, 16)

Insyn och transparens har genom offentlighetsprincipen länge erkänts vara det bästa sättet att förmå offentlig förvaltning att över tid förbättra och effektivisera handläggningen av enskilda ärenden, samt rättssäkerheten med vilken handläggningen sker. Samma princip gäller för informationssäkerhet och dataskydd, och därför bör varken brottsdatalagen eller brottsdataförordningen lämna utrymme för hemlighållande av säkerhetsproblem från privatpersoner annat än i väl definierade undantagsfall.

Varken NISU-utredningen,[93] Informationssäkerhetsutredningen,[94] Säkerhetsskyddsutredningen[95] eller Brottsdatalagsutredningen har lyckats klargöra exakt under vilka omständigheter nationens intresse av att hålla säkerhetsproblem hemliga ska ges företräde över enskilda privatpersoners möjligheter att skydda sig mot negativa verkningar av inträffade säkerhetsproblem. Säkerhetsskyddsförordningens 10a § och 39 § är vaga.[96] Till exempel finns inga krav på att det ska upprättas en lista över sådana viktiga system och vem som i sådana fall är ansvarig för underhållet av den listan. Enligt uppgift från Justitiedepartementet



Svarta lådan. Värdekedjorna i den digitala ekonomin och förvaltningen är redan väldigt komplicerade och svåra att bena ut. Vem som gör vad, vem som gör fel och vem man ska hålla ansvarig är inte lätt att reda ut. Om privatpersoners möjligheter att få information begränsas godtyckligt, blir privatpersoners ställning i den digitala ekonomin och förvaltningen väldigt svag. Därför anser inte Dataskydd.net att man ska undanhålla privatpersoner möjligheten att få reda på när informationssäkerhetsproblem inträffat som kan beröra privatpersonerna.

[93] SOU 2015:23.
[94] SOU 2017:36.
[95] SOU 2015:25.
[96] I säkerhetsskyddsförordning (1996:633) finns följande beskrivning av vilken sorts incidenter som privatpersoner inte har någon rätt att få reda på, till följd av att de anses mindre viktiga än riket:

10 a § En myndighet ska skyndsamt anmäla till den myndighet som enligt 39 § utövar tillsyn över säkerhetsskyddet om det inträffat en it-incident i myndighetens informationssystem och

1. incidenten allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa,

2. incidenten allvarligt kan påverka säkerheten i ett informationssystem som särskilt behöver skyddas mot terrorism, eller

3. incidenten upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt.

kan vilken som helst av myndigheterna när som helst på egen hand bestämma att den är så viktig att den är mer viktig än privatpersoners rätt till insyn i deras datasäkerhet.

Privatpersoner kan när som helst beslutas vara allt för oviktiga för staten för att få veta när saker som angår dem och drabbar dem inte får komma till privatpersonernas kännedom. Detta har en mycket begränsande inverkan på privatpersoners möjligheter att skydda och utöva sina rättigheter till privatliv och dataskydd. Informationsasymmetrin i informationssamhället är redan mycket stor till privatpersoners och konsumenters nackdel. Den sorts reglering som föreslås här är inte hjälpsam för att jämna ut den maktobalansen.

Vi föreslår därför att det ska upprättas en uttömmande lista över de system för vilka privatpersoners rätt att få reda på när de har utsatts för dataskyddsrisker ska falla bort till följd av att nationens intresse väger tyngre än privatpersonernas egna intresse.

Vi är kritiska mot att personuppgiftsansvariga själva får bedöma huruvida en incident ska anmälas till tillsynsmyndigheten eller inte i förslaget att incidenter inte ska anmälas när de inte medför en risk för otillbörligt intrång i privatpersons integritet. Det är mycket svårt för en brottsbekämpande myndigheten att självständigt bedöma när de gjort intrång eller riskerat att det begås intrång, i någon annans privatliv och dataskydd. De flesta står sitt egna privatliv och sin egen rätt till integritet närmast, och underskattar andras behov av privatliv och integritet. Därför finns en påtaglig risk att intrång kommer att begås eller kunna begås i privatpersoners integritet utan att vare sig tillsynsmyndigheterna eller privatpersonerna själva kan göra någonting åt det.

Det är inte heller möjligt för vare sig tillsynsmyndigheten eller privatpersonerna själva att självständigt och utan medverkan från de personuppgiftsansvariga etablera om det skett en incident eller hur pass allvarlig eller riskfylld incidenten i sådana fall har varit. Både tillsynsmyndigheten och privatpersoner är beroende av den personuppgiftsansvariges och personuppgiftsbiträdets omdömen. Dessa omdömen kan i sin tur antas fördunklas av det faktum att det normalt är svårt, inte bara för personuppgiftsansvariga under Brottsdatalag utan i allmänhet, att uppskatta andras behov av integritet, privatliv och dataskydd.

Dataskydd.net har vid ett antal andra tillfällen framhållit att högre transparens gentemot privatpersoner vid IT-säkerhetsproblem inte bara är en bra och stärkande åtgärd för privatpersonernas egna möjligheter att utöva sin rätt till dataskydd, utan också ett gott ekonomiskt och praktiskt incitament för företag och myndigheter att förbättra sin IT-säkerhet.[97] Sådana synpunkter som vi tidigare lyft fram är fortfarande giltiga och vi föreslår ändringar i Brottsdatalag i enlighet med de synpunkterna.

Utredaren har lagt för stor vikt vid skrivningen ”i specifika fall” i artikel 13.2 i det underliggande direktivet. Som mycket EU-lagstiftning är direktivet om

Jag är jag. Det är lättare att förhålla sig till sitt eget privatliv än till andras, på samma sätt som det är svårt att förhålla sig till andras okunskap när man själv vet. Att alla står sig själva närmast är en av de sakerna som gör att dataskydd, verktyget för att själv utöva skydd för det egna privatlivet, är ett viktigt verktyg för enskilda. Godtyckliga inskränkningar av rätten att få veta saker om det egna dataskyddet gör privatpersoner väldigt svaga. Myndigheters anställda bör inte antas besitta övermänskliga superkrafter som låter dem frångå det mänskliga i att relatera bättre de egna rättigheterna än till andras.

Det är skönsmässigt vad som är ett ”informationssystem”, vad som är ”hemligt” i informationssystemet samt vad ”som inte är ringa”. Vilka ”informationssystem” som ”särskilt behöver skyddas mot terrorism” är också skönsmässigt. Normalt kan detta innefatta samtliga myndighetsdatorer vid varje tidpunkt på dygnet, eftersom alla myndigheter måste presumeras ägna sig åt något som är viktigt för nationen och dess medborgare (och om detta inte vore fallet, vad gör de?). Det är vidare bekymmersamt att privatpersoner skulle berövas sin rätt att få insyn i datasäkerhetsarbetet bara för att Försvarets radioanstalt varit inblandad i upptäckten av incidenten.

[97] Dataskydd.net remissyttrande över Ju2017/02002/L4, SOU 2016:41, SOU 2015:23. Samtliga tillgängliga på https://dataskydd.net/vara-remissvar

personuppgiftsskydd i de brottsbekämpande myndigheternas verksamhet en kompromissprodukt som ibland betyngs med ordalydelser som inte är helt nödvändiga eller enkla att tolka. Dataskydd.net tror att ”specifika fall” ska tolkas som ”sådana fall där informationen i föregående artikel inte är tillräcklig för att den registrerade ska kunna utöva sina rättigheter på ett fullgott sätt” snarare än som ”specifika fall inom de brottsbekämpande myndigheternas verksamhet”. Dataskydd.net:s uppfattning om orden ”specifika fall” finner stöd i direktivets andemening i övrigt och syftet med att från början ha en dataskyddslagstiftning.

I 4 kap. 2 § kan alltså orden ”i specifika fall” tas bort, eftersom ordföljden uppenbarligen är så pass komplicerad att tolka att den snarare verkar begränsande på privatpersoners möjligheter att utnyttja sina rättigheter än förstärkande.

Värdet av att införa en ny bestämmelse i 4 kap. 11 § om att den personuppgiftsansvarige får välja att vidta valfri åtgärd ur listan ”rättelse, radering eller begränsning av behandling” när en privatperson begärt någon av dessa åtgärder är tveksamt. Den övriga lagtexten i 4 kap. 9-10 §§ förtydligar redan hur begäranden om rättelse, radering eller begränsning av behandlingen ska hanteras.

Sammanfattning.

Tillstyrker: 11.2.2, 11.3.2, 11.3.4, 11.4.1, 11.4.2, 11.4.3, 11.5.2, 11.5.3, 11.5.4, 11.5.7, 11.5.8, 11.5.9, 16.3.2, 16.3.4, 16.3.5.

Tillstyrker delvis: 10.4.1, 10.4.3, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.3.1, 11.3.3, 16.3.3, 16.4.

Avstyrker: 10.4.2, 11.4.4.

Brottsdatalag 3 kap. 9 § 2 stycket stryks.

Brottsdataförordningen 3 kap. 9 § kompletteras med texten ”Tillsynsmyndigheten ska underhålla en offentlig lista med sådana databehandlingssystem eller verksamheter för vilka privatpersoner inte kan erhålla information om personuppgiftsincidenter.”

Brottsdatalag 3 kap. 10 § 1 stycket ändras till ”Om en personuppgiftsincident som ska anmälas enligt 9 § första stycket *har inträffat,* ska den personuppgiftsansvarige *som huvudregel* utan onödigt dröjsmål underrätta den registrerade om incidenten.”

I Brottsdatalag 4 kap. 2 § tas orden ”i specifika fall” bort, eftersom de inte bidrar till klarhet kring vad de ytterligare informationsförpliktelserna är menade att uppnå.

Brottsdatalag 4 kap. 11 § tas bort. De tillför ingenting till 4 kap. 9-10 §§.

Brottsdatalag 4 kap. 6 § 1 stycket kompletteras med texten ”, om inte den registrades intresse av att kunna utöva sina rättigheter väger tyngre än myndighetens intresse av att inte lämna ut informationen.”

Vad händer med överskottsinformation?

Vid användning av hemliga tvångsmedel samlar de brottsbekämpande myndigheterna in personuppgifter i stora mängder, och ofta sådana personuppgifter

som inte är direkt relaterade till brottsligheten de hade avsikt att utreda med hjälp av det hemliga tvångsmedlet.

Utredaren har inte lyft frågan om vad som gäller för information och överskottsinformation som samlats in med hjälp av hemliga tvångsmedel, men det är Dataskydd.net:s bestämda uppfattning att personuppgifter som samlas in på sådant sätt inte ska åtnjuta ett lägre eller sämre skydd än andra personuppgifter som hanteras i de brottsbekämpande myndigheternas verksamhet.

Lagstiftningen om hemliga tvångsmedel reglerar framför allt hur personuppgifter kan samlas in, men inte den efterföljande behandlingen. Det vore olyckligt om man kan vara extra slapphänt med datasäkerheten eller strunta i att rapportera personuppgiftsincidenter bara för att man använt sig av hemlig teleövervakning eller hemlig teleavlyssning för att samla in personuppgifterna i stället för att samla in personuppgifterna på något annat sätt.

Dataskydd.net har också föregående år påtalat att reglerna om överskottsinformation så som de tillämpas i Sverige idag inte är särskilt väl anpassade till den sortens hemliga tvångsmedel de brottsbekämpande myndihgeterna föreställer sig att använda i framtiden.[98] Eftersom den sortens ingrepp i privat kommunikation som de brottsbekämpande myndigheterna vill ägna sig åt nu för tiden är av en mycket med djuplodande och genomträngande karaktär än tidigare tvångsmedel kunnat uppnå, samtidigt som möjligheten att via inferenser, profilering och allmänna kontroller bedöma medborgare på bas av den informationen dramatiskt ökat, menar vi att det krävs en skärpning av reglerna för hantering av överskottsinformation.

Amelia Andersdotter
Ordförande, Dataskydd.net

[98] Dataskydd.net och DFRI:s inlagor till utredningarna om modernisering av beslag och husrannsakan (Beslagsutredningen) och hemlig dataavläsning.

Källförteckning

Rättskällor och offentliga tryck

1. Datainspektionen, Dnr 1546-2016 om tillsyn enligt personuppgiftslagen (1998:204) – behörighetstilldelning, spärrar m.m enligt patientdatalagen riktad mot Hälso- och sjukvårdsnämnden i Region Gävlebord. http://www.datainspektionen.se/Documents/beslut/2017-04-25-region-gavleborg.pdf
2. ECLI:EU:C:2003:596, C-101/01. Barbro Lindqvist. http://curia.europa.eu/juris/documents.jsf?num=C-101/01
3. ECLI:EU:C:2010:125, C-518/07. Kommissionen. http://curia.europa.eu/juris/documents.jsf?num=C-518/07
4. ECLI:EU:C:2012:631, C-614/10. Kommissionen. http://curia.europa.eu/juris/documents.jsf?num=C-614/10
5. ECLI:EU:C:2014:237, C-288/12. Kommissionen. http://curia.europa.eu/juris/documents.jsf?num=C-288/12
6. ECLI:EU:C:2014:238, C-293/12. Digital Rights Ireland. http://curia.europa.eu/juris/documents.jsf?num=C-293/12
7. ECLI:EU:C:2015:639, C-230/14. Weltimmo. http://curia.europa.eu/juris/liste.jsf?num=C-230/14
8. ECLI:EU:C:2015:650, C-362/14. Maximilian Schrems. http://curia.europa.eu/juris/documents.jsf?num=C-362/14
9. ECLI:EU:C:2016:656, Yttrande 1/15, punkt 222, föredraget 8 september 2016. http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=SV&mode=lst&dir=&occ=first&part=1&cid=322111
10. ECLI:EU:C:2017:222, C-203/15. Tele2. http://curia.europa.eu/juris/documents.jsf?num=C-203/15
11. Europeiska domstolen för mänskliga rättigheter, Grand Chamber, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (Application no. 931/13). http://hudoc.echr.coe.int/eng?i=001-175121
12. Post- och telestyrelsen, Årsredovisning 2016 (PTS-ER-2017:01). https://www.pts.se/upload/Rapporter/Om-PTS/pts-arsredovisning-2016.pdf
13. Regeringen, Skrv. 2009/10:79, En tydlig, rättssäker och effektiv tillsyn. http://tillsynsforum.se/wp-content/uploads/2013/12/En_tydlig_rattssaker_och_effektv_tillsyn_Regeringens_skrivelse_2009-10-79.pdf
14. Regeringen, Proposition 2016/17:198, Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring . http://www.regeringen.se/49f006/contentassets/696b5453fb0c427fbdc45290c73df5ae/utokat-sekretesskydd-i-verksamhet-for-teknisk-bearbetning-och-lagring-prop.-201617198.pdf
15. Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D). http://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf
16. SOU 2015:23, Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201523/
17. SOU 2015:25, En ny säkerhetsskyddslag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201525/
18. SOU 2015:39, Myndighetsdatalag http://www.regeringen.se/contentassets/f07ea73b5c11475ebb7fe4468703baa7/myndighetsdatalag-sou-201539
19. SOU 2015:73, Personuppgiftsbehandling på utlännings- och medborgarskapsområdet http://www.regeringen.se/4a21c2/contentassets/f238f9a7c211483b990a35de3ffa15c1/personuppgiftsbehandling-pa-utlannings--och-medborgarskapsomradet-sou-201573
20. SOU 2016:41, Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén http://www.regeringen.se/49c627/contentassets/13d9126efbb94e2cb5b084132275f184/hur-star-det-till-med-den-personliga-integriteten---en-kartlaggning-av-integritetskommitten-sou-201641

21. SOU 2016:65, Ett samlat ansvar för tillsyn av den personliga integriteten http://www.regeringen.se/4a7e12/contentassets/f1c405e7cdb645bca480326f10f3b809/sou_2016_65_webb.pdf
22. SOU 2017:36, Informationssäkerhet för samhällsviktiga och digitala tjänster. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2017/05/sou-201736/
23. SOU 2017:39, Ny dataskyddslag http://www.regeringen.se/49a184/contentassets/e98119b4c08d4d60a0a2d0878990d5ec/ny-dataskyddslag-sou-201739
24. SOU 2017:52, Så stärker vi den personliga integriteten http://www.regeringen.se/49c6b6/contentassets/56e701d354824bcb9826ea0839ab28f3/sa-starker-vi-den-personliga-integriteten-sou-2017-52.pdf

Övriga källor

1. Dataskydd.net, Remissyttrande över SOU 2015:23. https://dataskydd.net/sites/default/files/sou201523_remissyttrande_dataskyddnet.pdf
2. Dataskydd.net, Remissyttrande över SOU 2015:25. https://dataskydd.net/sites/default/files/sou201525_remissyttrande_dataskyddnet.pdf
3. Dataskydd.net, Remissyttrande över SOU 2015:39. https://dataskydd.net/sites/default/files/sou201539_remissyttrande_dataskyddnet.pdf
4. Dataskydd.net, Remissyttrande över Ds 2016:31. https://dataskydd.net/sites/default/files/ds201631_remissyttrande_dataskyddnet_20161216.pdf
5. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI), Remissyttrande över promemorian Ju2017/02002/L4 om ett tekniskt sensorsystem hos MSB. https://dataskydd.net/sites/default/files/dfri_dataskyddnet_promemoriaju201702002l4_utan_sig.pdf
6. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om hemlig dataavläsning. https://dataskydd.net/sites/default/files/dir201636_dfri_dataskyddnet_slutgiltig_2.pdf
7. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan. https://dataskydd.net/sites/default/files/dir201620_dfri_dataskydd_slutgiltig.pdf
8. Engelin, M. och de Silva, F., Troll Detection – A comparative study in detecting troll farms on Twitter using cluster analysis, Kandidatuppsats i datavetenskap, KTH, 2016. http://www.diva-portal.org/smash/get/diva2:927209/FULLTEXT02
9. Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion?, 6 januari 2016, USA:s regering. https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf
10. UFC-Que Choisir (9 juni 2014) ”*Action de groupe – Du nouveau!*” https://www.quechoisir.org/enquete-action-de-groupe-du-nouveau-n3689/
11. Zuiderveen Borgesius, Frederik J., Online Price Discrimination and Data Protection Law (August 28, 2015). Amsterdam Privacy Conference 23-26 October 2015; Amsterdam Law School Research Paper No. 2015-32; Institute for Information Law Research Paper No. 2015-02. https://ssrn.com/abstract=2652665 och http://dx.doi.org/10.2139/ssrn.2652665