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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

2016-06-10, Bryssel

Brister i Europarlamentets 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)

Inledning

Förordning (EU) 2016/679.

Den allmänna dataskyddsförordningen har till syfte att harmonisera behandlingen av personuppgifter i Europeiska unionen och göra det enklare och mer förutsägbart för marknadens aktörer, konsumenter och enskilda vilka rättigheter och skyldigheter de har i givna lägen. Förordningen kan tänkas bidra till enklare upphandlingsförfaranden, då kraven som ställs på IT-systemens utvecklare kommer att vara liknande i hela unionen.

Förordningen har dock ett större antal undantag än det tidigare direktivet hade artiklar, närmare bestämt 61 undantag mot det tidigare direktivets 34 artiklar. Dessa undantag återfinns i artiklarna 4(7), 4(9), 6(2), 6(3)(b), 6(4), 8(1), 8(3), 9(2)(a), 9(2)(b), 9(2)(g), 9(2)(h), 9(2)(i), 9(2)(j), 9(3), 9(4), 10, 14(5)(b), 14(5)(c), 14(5)(d), 17(1)(e), 17(3)(b), 17(3)(d), 22(2)(b), 23(1)(e), 26(1), 28(3), 28(3)(a), 28(3)(g), 28(3)(h), 28(4), 29, 32(4), 35(10), 36(5), 37(4), 38(5), 49(1)(g), 49(4), 49(5), 53(1), 53(3), 54(1), 54(2), 58(1)(f), 58(2), 58(3), 58(4), 58(5), 59, 61(4)(b), 62(3), 80, 83(5)(d), 83(7), 83(8), 85, 86, 87, 88, 89, 90.[1]

Av dessa rör 11 registerforskning och statistik, 26 rör möjligheter för medlemsländer att ändra enskildas rättigheter enligt förordningen, 10 rör ansvarsfördelning mellan de aktörer som påverkar enskilda och därför enskildas rätt att utöva sina rättigheter enligt förordningen och 15 rör administrativa förhållande rörandes tillsyn. Anledningen till att detta blir 62 undantag är för att artikel 14(5)(b) innebär både ett undantag för registerforskning och statistik, samt ett undantag för tillfällen då så kallade intresseavvägningar måste redovisas för enskilda.

Denna text fokuserar på medlemsstaternas befogenhet att särreglera dataskydd i nationell rätt. Rättigheter som medlemsstaterna inte kan särreglera kommer att uttolkas av tillsynsmyndigheterna (Datainspektionen och den europeiska samarbetsgruppen för dataskyddsmyndigheter: Artikel 29-gruppen/European Data Protection Board) och av domstolar, i slutändan EU-domstolen. Mängden dataskyddsrelaterade rättstvister som når EU-domstolen har redan stadigt ökat, och kan förväntas öka ännu mer efter det att de större möjligheterna för administrativa sanktionsavgifter träder i kraft 2018.

[1] Amberhawk Training (4 maj 2016) ”How ’flexible’ can the UK actually be on EU data protection law?”, The Register.

Övriga brister i dataskyddsförordningen, till exempel då den europeiska lagstiftaren varit otydlig eller har begränsat möjligheten för enskilda att utöva sina rättigheter effektivt, berörs inte i denna text i den utsträckning svenska lagstiftare inte själva kan påverka stärkande av rättigheterna.

För nätbaserade resurser finns i slutet av dokumentet en lista med länkar till källhänvisningarna i fotnötterna.

Den här texten är upplagd på följande sätt: olika funktioner i förordningen behandlas (rättigheternas substans, undantag, ansvar, administration, sanktioner). Vi har ett särskilt avsnitt för två frågeställningar kring artikel 23, som rör undantag från dataskydd. Dessa går utöver den ovanstående undantagslistan.

I allmänhet tror vi att riksdagen skulle vara hjälpt av följande saker:

- Regeringen bör redovisa i propositioner vilka specifika undantag i dataskyddsförordningen de stödjer sig på för att införa begränsningar av enskildas rätt till dataskydd. Detta kommer underlätta riksdagens granskning av förslagen.
- Riksdagen kan ta ett mer aktivt intresse för Datainspektionens arbete, både så till vida att man kan gå igenom sådant Datainspektionen redan har gjort, men också så att man kontinuerligt (via tematiska hearings) informerar sig om Datainspektionens kommande planer.

Rättigheternas substans

Nedan utvecklas kritik mot kryphålet för berättigade intressen (intresseavvägningar) i artikel 6(1)(f) och artikel 14(5)(b)), kryphålet för bevarande av nationella registerförfattningar i artikel 6(2), och kryphålen för statistik, forskning och hälsa i artiklarna 5(1)(b), 5(1)(e), 9(2)(c), 9(2)(h), 9(2)(j), 9(4), 14(5)(b), 17(3)(d), 21(6), 23(e), och 89. Det finns flera andra artiklar som tillåter medlemsländerna att försvaga individers rättigheter genom nationell lagstiftning (t ex artikel 85-88 samt artikel 91) som inte behandlas nedan.

Förordningens ”ramverk”

Rättigheternas substans finns i kapitel I-IV i förordningen. De mest generella principerna återfinns i artikel 5 och är laglighet, korrekthet och öppenhet (5(1)(a)), ändamålsbegränsning (5(1)(b)), uppgiftsminimering (5(1)(c)), korrekthet (5(1)(d)), lagringsminimering (5(1)(e)), integritet och konfidentialitet (5(1)(f)) och ansvarsskyldighet (5(2)).

Notera att förordningens svenska översättning använder begreppet ”korrekthet” för två separata principer. På engelska motsvaras begreppen av ”fairness” (5(1)(a)) och ”accuracy” (5(1)(d)).[2] På franska motsvaras begreppen av ”loyauté” (5(1)(a)) och ”exactitude” (5(1)(d)),[3] och på tyska ”Verarbeitung nach Treu und Glauben” (5(1)(a)) respektive ”Richtigkeit” (5(1)(d)).[4] Vi kan alltså vara säkra på att begreppet ”korrekthet” har olika innebörd i artikel 5(1)(a) och artikel 5(1)(d). Artikel 5(1)(a) syftar mer till att göra det rättvist och begripligt vad som händer, medan artikel 5(1)(d) tar sikte på att uppgifterna ska vara rätta och beskriva

[2] Regulation (EU) 2016/679.
[3] Règulation (UE) 2016/679.
[4] Verordning (EU) 2016/679.

faktiska omständigheter (så att man till exempel inte blir bedömd på felaktig grund).

Den exakta innebörden av dessa principer finns i senare artiklar. Till exempel regleras öppenhet (på engelska ”transparency”) i artiklarna 12-15. Korrekthet (”accuracy”) regleras närmare i artikel 16 och artikel 22. Ändamålsbegränsning, lagringsminimering och uppgiftsminimering kan sägas genomsyra bestämmelserna i artiklarna 17-20 (men även bestämmelser i övrigt). Integritet och konfidentialitet ska säkerställas genom bestämmelserna i kapitel IV samt bestämmelserna om incidentrapporting i artiklarna 33-34.

I artikel 6 i dataskyddsförordningen finns bestämmelser om ”juridiska baser” för personuppgiftsbehandling, det vill säga, när man uppfyller laglighetskravet i artikel 5(1)(a). Dessa baser är: samtycke (6(1)(a)), fullgörande av avtal (6(1)(b)), juridisk skyldighet (6(1)(c)), skydd av annans intressen (6(1)(d)), del av myndighetsutövning (6(1)(e)), berättigade intressen (6(1)(f)).

Det här innebär till exempel att en myndighet, i enlighet med förordningens principer och regler, får behandla personuppgifter i sin verksamhet (artikel 6(1)(e)). Om en konsument har beställt en produkt som ska levereras hem till konsumenten, får handlaren behandla namn- och adressuppgifter eftersom detta är en förutsättning för att varan ska levereras (artikel 6(1)(b)). Har man en skyldighet att motverka bedrägerier får man av detta skäl behandla personuppgifter (artikel 6(1)(c)). Om inga av de ovanstående omständigheterna gäller, måste man ha samtycke från privatpersonen. I praktiken baseras de flesta behandlingar av personuppgifter i till exempel amerikanska nättjänster på samtycke. I arbetslivet har det varit vanligt att Datainspektionen godkänner behandling för berättigade intressen.[5]

Kryphål: Berättigat intresse (artikel 6(1)(f); artikel 14(5)(b))

Det berättigade intresset i artikel 6(1)(f) är ett stort kryphål i förordningen. Den ger en rätt att behandla uppgifter när detta är ”nödvändig[t] för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter”.

I praktiken finns inga möjligheter för enskilda att förstå när något företag de varit i kontakt med kan ha varit i kontakt med ytterligare ett företag som privatpersonen inte känner till och som i sin tur upplever sig ha intressen som är viktigare än privatpersonens grundläggande rättigheter. Bara en mening som beskriver denna relation är i sig själv svårbegriplig.

I artikel 14 finns bestämmelser om information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade som mildrar konsekvenserna av artikel 6(1)(f).

Med tillräcklig tillsynsverksamhet blir det svårt för tredjeparter från näringslivet som inte haft direkt kontakt med en privatperson att göra intresseavvägningar i smyg. Enskilda blir dock helt utelämnade åt den mängd resurser som tillsynsmyndigheten kan avvara för tillsyn, och kanske inte heller får tillräcklig information om när och hur intresseavvägningar har gjorts.

Ett kryphål i artikel 14(5)(b) gör att *bara* tillsynsverksamheten har tillräckliga

[5] Se kapitel 8, SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen.

verktyg för enskilda att hävda sina rättigheter att göra invändningar (artiklarna 15, 21-22): en näringslivsaktör måste inte berätta vad den gör för en enskild om den upplever att den genom att tala om vad den gör och varför riskerar att inte kunna utföra behandlingen och åtnjuta behandlingens fördelar.

Integritetskartläggningen 2016[6] visar på flera ställen, men särskilt i förhållande till integritetsskydd i arbetslivet, att personuppgiftslagens befintliga bestämmelser om berättigat intresse i praktiken används för att komma runt att det inte går att inhämta samtycke för personuppgiftsinsamling och -behandling. Bestämmelsen riskerar alltså fortsätta vara en ”catch-all”-bestämmelse som alltid går att falla tillbaka på när man inte i övrigt har fog för det man gör.

Förslag: Datainspektionen är den enda aktör som genom möjligheten att bedriva tillsyn och genomföra inspektioner kan kompensera för det bortfall av rättigheter som individer kan utsättas för i och med bestämmelserna i artikel 6(1)(f) och 14(5)(b). Riksdagen bör se till att Datainspektionen får tillräckliga resurser, och egen teknisk kompetens (till exempel ett tekniskt labb så som hos CNIL eller dataskyddsmyndigheten i Schleswig-Holstein).

Kryphål: Registerförfattningar (artikel 6(2))

Artikel 6(2) ger möjligheter för medlemsländer att behålla eller fastställa befintliga registerförfattningar. I Sverige är registerförfattningarna många och ogenomträngliga.[7] De är också detaljerade och begränsar både myndigheternas verksamhet och deras förutsättningar att förändra eller bygga ut eller om sin informationsteknologiska infrastruktur.[8] Varje typ av förändring i myndigheternas informationsteknologiska infrastruktur kräver i princip först en lagändring, oavsett om förändringen i själva verket skulle innebära bättre dataskydd eller inte.[9]

I praktiken leder de svenska registerförfattningarna också till att bara myndigheterna själva har kapacitet att förstå och hålla koll på vilka rättigheter enskilda har, och vilka skyldigheter den egna verksamheten har. Utredningen om en ny myndighetsdatalag[10] som kom våren 2015 tog över fyra år att sammanställa, vilket borde ses som en indikation på att inte ens regeringen och riksdagen i praktiken har möjlighet att effektivt tillse och uppdatera registerförfattningarna å privatpersoners vägnar.

Svenska regeringen kommer att hänvisa till artikel 9 med förbudsbestämmel-

[6] SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen.

[7] På s. 165 i SOU 2012:90 Överskottsinformation vid direktåtkomst talar kommittéen om den ”splittrande och föråldrade strukturen i de nuvarande registerförfattningarna”.

[8] Se t ex Digitaliseringskommissionens behandlingar av sekretess- och direktåtkomstbestämmelser.

[9] s. 79, SOU 2016:31:

> ”En generell iakttagelse som kommittén gör, är dock att myndigheter och regeringen fokuserar sitt utvecklings- och författningsarbete på [att öka spridningen och vidareanvändningen av uppgifter], medan man arbetar betydligt mindre på [att skydda uppgifterna på ett bättre sätt genom att använda tekniker som stärker den personliga integriteten, t.ex. anonymisering]. Det innebär att offentlig sektor riskerar att bygga in egenskaper i system, arbetsformer och i författningar, som kan bli mycket svåra och dyra att ändra på, om följderna för den personliga integriteten visar sig bli allvarliga.”

[10] SOU 2015:39 Myndighetsdatalag.

ser mot att behandla uppgifter av känslig karaktär (ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning) för att få behålla registerförfattningarna. Artiklarna 9(1)(f), 9(1)(h) och 9(1)(i) lämnar dock redan öppet för behandling av känsliga uppgifter i domstolsväsendet och i hälsosyfte. Regeringen kommer att lyfta artikel 9(1)(g) som skäl för att ha kvar registerförfattningarna (viktigt allmänt intresse med särskilda skyddsåtgärder), men ett mer uppenbart sätt är att förlita sig på samtycke under artikel 9(1)(a): frågan är om myndigheter verkligen behöver kartlägga enskildas sexualitet, ras, etnicitet, politiska åsikter och religiösa övertygelser utan att enskilda godkänner detta. Enligt mig är skälen för detta inte starka.

Förslag: Den svenska lagstiftaren bör minska det svenska beroendet av artikel 6(2) för att istället se till att myndigheternas verksamhet är tillräckligt väl reglerad för att myndigheterna ska kunna förhålla sig till dataskyddsförordningens allmänna bestämmelser enligt artikel 6(1)(e). Större transparens krävs istället kring myndigheternas behandling av känsliga personuppgifter, och myndigheternas verksamhet behöver inte utformas efter antagandet att medborgarna ska misstro myndigheterna och vägra låta myndigheterna genomföra sitt jobb effektivt.

Kryphål: statistik, forskning och arkivering (många olika artiklar)

Möjligheter för medlemsländer att införa ett sämre skydd för enskilda (minskade möjligheter att avge samtycke, invända, informeras och begränsa personuppgiftsbehandling) för syften som rör statistisk, forskning, arkivering eller hälsa finns i artiklarna 5(1)(b), 5(1)(e), 9(2)(c), 9(2)(h), 9(2)(j), 9(4), 14(5)(b), 17(3)(d), 21(6), 23(e), och 89.

Sveriges regering har under hela förhandlingsprocessen uttryckt ett starkt stöd för dessa möjligheter till nationella undantag på grund av registerforskningens traditionellt starka ställning i Sverige. Omständigheterna kring behandling av personuppgifter i svenska sjukvård har upprepade gånger fått kritik av Datainspektionen.[11] Även Integritetskommittéen 2016 lyfter problem med integritetsskyddet i vårdsammanhang, forskning och statistik.[12]

Om integritetsskydd för enskilda kommer i vägen för forskning som är tilltänkt, ändras den svenska lagstiftningen - snabbt.[13] Integritetskommittéen är inte klara med om det saknas utredningar av dataskydds- och datasäkerhetsa-

[11] Datainspektionen (8 juni 2016) ”Vårdgivare måste förhindra att anställda får för vid åtkomst till journaluppgifter”; Datainspektionen (26 oktober 2015) ”Allvarlig kritik mot bristfällig utredning på e-hälsoområdet”; Datainspektionen (8 juli 2015) ”Tydligare information krävs vid forskningsstudier”; Datainspektionen (27 april 2015) ”Tillfällig forskningslag bör inte förlängas”; Datainspektionen (12 februari 2015) ”Kritik mot lagförslag för registerbaserad forskning”.

[12] Kapitel 7.4, 9 och 10, SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen.

[13] Datainspektionen (19 december 2011) ”Forskningsprojektet LifeGene är olagligt och måste upphöra”; Datainspektionen (3 juli 2012) ”Skarp kritik mot förordning för befolkningsbaserad forskning”

I ett yttrande riktar Datainspektionen skarp kritik mot det förslag till förordning som lagts fram för att göra omfattande befolkningsbaserad forskning som exempelvis LifeGene möjlig.

spekter vid myndigheternas statistikframställning,[14] eller om det har genomförts utredningar som inte visar några problem med statistik behandling. Kommittéen beskriver i alla fall att Statistikutredningen kommit fram till att myndigheterna inte alltid vet vilken statistisk verksamhet de genomför.[15] Under våren 2016 har regeringen föreslagit att ge biobanker, inklusive PKU-registrena, nya syften.[16] Mycket av särregleringen kommer på grund av förordningens många undantag att ligga kvar på nationell nivå.

Förslag: 1) Individer kan ges SMS-notifikationer, brev eller dylikt kan användas för att aktivt informera individer om att deras information ska spridas inom vårdverksamhet eller för forskningssyfte. Landstingen kan redan skicka räkningar, och borde kunna skicka datatillgångsmeddelanden också. 2) Landstingen bör åläggas att tydligt informera individer om att de har rätt att begära att prover förstörs. Denna skyldighet bör inte åläggas personalen utan finnas tillgänglig på vårdcentraler i form av utdelnignsmaterial (till exempel). 3) Det ska vara tydligt när och om ens uppgifter lämnas ut till forskning eller statistisk behandling, samt vilka individer som i sådana fall ansvarar för forskningen och den statistiska behandlingen. 4) Idag saknas enkla möjligheter för ansvarsutkrävande, vilket skapar illusionen för forskare om att ingen påverkas av deras handlingar och illusionen för enskilda om att ingenting händer. Arkiveringsmaterial bör i så stor utsträckning som möjligt avidentifieras.

Undantag

I artikel 23 dataskyddsförordningen kodifieras nio situationer där medlemsländerna får göra undantag från dataskyddsförordningens bestämmelser. Dessa innefattar: den nationella säkerheten (23(1)(a)), försvaret (23(1)(b)), den allmänna säkerheten (23(1)(c)), förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten (23(1)(d)), andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet (23(1)(e)), skydd av rättsväsendets oberoende och rättsliga åtgärder (23(1)(f)), förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken (23(1)(g)), en tillsyns-, inspektions- eller regleringsfunktion (23(1)(h)), skydd av den registrerade eller andras rättigheter och friheter (23(1)(i)) samt verkställighet av civilrättsliga krav (23(1)(j)).

Datainspektionen yttrar sig nu om ett förslag till förordning om ”register för viss befolkningsbaserad forskning” som tagits fram av regeringen. I sitt yttrande riktar myndigheten skarp kritik mot förslaget.

[14] s. 78, SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen.

[15] s. 280–281, SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen.

[16] Dir. 2016:41 En ändamålsenlig reglering för biobanker.

Svaghet: Dåliga definitioner (23(1)(a), (23(1)(b), (23(1)(c))

Begreppet ”nationell säkerhet” har redan påtalats sakna en bra definition av Artikel 29-gruppen.[17] I artikel 23 är det dessutom otydligt vad som skiljer ”nationell säkerhet” från ”försvar” och ”allmän säkerhet”. Det implicerar att nationen och allmänheten inte är samma sak, och att nationens och allmänhetens säkerhetsintressen kan gå isär.

Svaghet: Förvirrande undantag (23(1)(d))

I artikel 23(1)(d) står det att medlemsländerna får införa undantag för förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. I artikel 2(2)(d) framgår dock att förordningens bestämmelser inte alls gäller för personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Det är svårt att tolka skrivningen i artikel 23(1)(d) på något annat sätt än att det funnits en avsikt att ge aktörer som inte är myndigheter möjligheter att utföra brottsbekämpande aktiviteter trots förordningen.

Förslag: Det finns inte mycket annat att göra än att vara vaksam på när svenska regeringen försöker anta lagstiftning med hänvisning till undantagen i dataskyddsförordningens artikel 23. Hänvisningar till artikel 23 kommer att framgå antingen i de förberedande statliga offentliga utredningarna, eller i bästa fall i den för lagstiftningen föregående propositionen. Riksdagen kan underlätta sitt arbete att granska regeringens motiveringar för dataskyddsinskränkande lagstiftning genom att kräva att regeringen redovisar undantagen i propositionerna.

Ansvar

Medlemsländerna har möjlighet att korrigera ansvarsfördelningen mellan enskilda, företag och myndigheter i artiklarna 26(1), 28(3)(a), 28(3)(g), 28(4), 29, 32(4), 35(10), 37(4), 80 ooch 83(8). Efter artikel 80 och 83(3) behandlas i avsnittet om sanktioner nedan behandlas de inte vidare här.

De övriga artiklarna ger medlemsländerna en möjlighet att via lagstiftning flytta ansvar mellan olika parter, eller undanta parter från ansvar med hjälp av ansvar. Till exempel kan ett delat personuppgiftsansvar leda till att informationskraven i artikel 13 och 14 (rätten att få reda på hur, varför och när uppgifter samlas in, samt varifrån) inte behöver följas (artikel 26(1)). Detta är dåligt för enskilda eftersom det blir svårare för dem att hålla rätt på exakt vilken rätt till information de har i olika lägen.

I artikel 29 ges vidare en möjlighet för medlemsländerna att via egen lagstiftning ge tredjeparter skyldigheter att behandla, sprida och samla in uppgifter, återigen med risk för att enskilda får sämre information om hur deras uppgifter sprids.

[17] s. 14 Artikel 29-gruppen, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes.

I artikel 32(4) får medlemsländerna via lagstiftning minska säkerhetskraven för underleverantörer, på ett sätt som gör det svårt för enskilda att hålla reda på vem som har vilka skyldigheter vid vilken tidpunkt.

Enligt artikel 35(10) är det inte tydligt att myndigheter som behandlar personuppgifter med stöd av en registerförfattning måste göra konskvensanalyser och risk- och sårbarhetsanalyser för sina informationsteknologiska system. Istället verkar förordningen förutsätta att lagstiftaren har gjort detta när den arbetade med lagstiftningen. Det är emellertid osannolikt att lagstiftaren har rätt kompetens att utföra ett sådant arbete redan i lagstiftningsprocessen, och bristande risk- och sårbarhetsanalyser hos svenska myndigheter är redan ett stort skäl till att informationssäkerhetsarbete inte fungerar på myndigheterna.[18]

Ansvarsförflyttningarna i artikel 28 (vilka avtal som måste upprättas mellan olika parter) och artikel 37 har inte nödvändigtvis någon större inverkan på enskildas rättigheter, om inte artikel 37 tolkas på ett sådant sätt att större organisationer (stora företag och myndigheter) undantas från kravet på att en person ska utses som är ansvarig för dataskydd inom företagets eller myndighetens verksamhet.

Förslag: Den svenska lagstiftaren bör inte försöka överta rollen att utföra risk- och sårbarhetsanalyser samt konsekvensanalyser för specifika tekniska lösningar. Registerförfattningar med detaljerade bestämmelser om hur myndigheternas IT-system ska fungera minskar flexibiliteten för myndigheterna, leverantörer och medborgare. Ett bra system för ansvarsutkrävande är viktigare och kan uppnås med bättre transparens, dataskyddsombud, incidentrapporter som hamnar hos enskilda drabbade istället för statistikansamlande myndigheter och bättre möjligheter för skadestånd och grupptalan (som inte underskrider i storlek kostnaden för juridiska ombud).

Administration

Administrativa korrigeringar rör företrädelsevis hur man utser myndighetschefer, styrande råd, representanter, dataskyddsombud eller samarbetsfunktioner mellan de svenska myndigheterna och de utländska. Möjligheter för medlemsländerna att avvika från förordningens bestämmelser finns i artiklarna 38(5), 53(1), 53(3), 54(1), 54(2), 58(1)(f), 58(2), 58(3), 58(4), 58(5), 59, 61(4), 62(3), 83(5)(d) och 83(7).

Här finns oftast en etablerad praktik i varje medlemsland. I Europeiska unionen som helhet har vissa yngre demokratier inte haft ett opolitiskt och självständigt utseende av myndighetschefer, vilket gjort att myndigheternas verksamhet varit mer följsamma med den sittande regeringen.

Sverige kan agera föredöme genom att göra en poäng av att ha opolitiska förfaranden för utseende av myndighetschefer och styrande råd.

Samtliga frågor om Datainspektionens funktionssätt har delegerats av regeringen till utredningen om tillsyn av personuppgiftsbehandling[19]. Detta inkluderar hur Datainspektionen ska arbeta, hur ansvariga personer ska utses, vilka resurser myndigheten ska ha, och vilka befogenheter myndigheter ska ha.

[18] Se nedan fotnot *a*.

[19] Utredningen om tillsynen över den personliga integriteten Ju 2015:02 etablerad av Dir. 2014:164.

I utredningsuppdraget för utredningen om dataskyddsförordningen[20] nämns få av artiklarna som reglerar möjligheterna för medlemsländerna att genomföra administrativa undantag. Man får anta att regeringen istället kommer att behandla dessa möjligheter i separata utredningar.

Möjligheten för anpassningar av nationell rätt i artikel 38(5) kan ha inverkan på hur enkelt det är för dataskyddsombud att utföra sitt jobb. Information om företags och myndigheters IT-system och personuppgiftsbehandling kan vara skyddad av industrirättigheter, så att dataskyddsombudets möjligheter att genomföra sitt jobb påverkas av vilka möjligheter de har att inte vidarebefodra saker de får veta. Det kan också hända att visselblåsare i en organisation vill påtala fel, men inte känner sig säkra på att de kan lyfta felen utan att drabbas av negativa konsekvenser. Då kan tystnadsplikt för dataskyddsombuden hjälpa arbetstagare känna sig trygga med att påtala fel.

Sanktioner

Den allmänna dataskyddsförordningen är utformad enligt vad man i svensk rätt kallar ”hanteringsmodell”. Den svenska lagstiftaren, och i stor utsträckning även den juridiska doktrinen, har istället inriktat sig på det man kallar en ”missbruksmodell”. Missbruksmodellen innebär att kränkande överträdelser av individuella rättigheter beivras när de upptäckts. Hanteringsmodellen innebär att insamling, bearbetning och spridning av uppgifter regleras på förhand.

Missbruksmodellen är inspirerad av amerikansk lagstiftning, där man i högre utsträckning än i EU har fokuserat på konsekvenser av missbruk genom att till exempel lagstifta mot diskriminering till följd av automatisk personuppgiftsbehandling. Den amerikanska lagstiftningen kan ta sikte på till exempel diskriminering till följd av personuppgiftsbehandling i försäkringsväsendet, långivarväsendet eller i sjukvården. USA saknar en heltäckande personuppgiftslagstiftning liknande den europeiska, även om det på senare år har föreslagits ett sådant ramverk (President Obamas Privacy Act 2012[21]) och höjts starkare röster för en mer omfattande reglering av personuppgiftsinsamling även i doktrin.

Till skillnad från i amerikansk doktrin finns i svensk rätt få verktyg att beivra faktiskt missbruk. Integritetsutredningen 2016 har hittat mycket få fall då skadestånd har utdömts och i praktiken inga fall då straffrättsligt skydd gjorts gällande.[22] Utredningen om integritet och straffskydd (”näthatsutredningen”) har dragit samma slutsats.[23] Det saknas både doktrinära och statliga behandlingar av frågan om huruvida de tillgängliga sanktionerna mot missbruk är tillräckliga och effektiva. EU:s Fundamental Rights Agency har noterat att sanktionerna vid överträdelser av dataskyddsbestämmelser i svensk rätt är förhållandevis låga.[24]

Att Sverige haft en amerikansk lagstiftningsteknik, men traditionellt svenska metoder för att upprätthålla lagstiftningen, innebär att uppföljningen av den

[20] Dir. 2016:15.

[21] Vita huset, ”We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consu- mers Online”, 23 februari 2012.

[22] Kapitel 6.8, SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen.

[23] s. 273 SOU 2016:7 Integritet och straffskydd.

[24] s. 21 Fundamental Rights Agency, Access to data protection remedies in EU Member States, januari 2014; s. 43 Fundamental Rights Agency, Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), komparativ studie, maj 2010.

svenska lagstiftningen varit dålig och incitamenten att följa lagstiftningen få. Det kan antas innebära särskilda utmaningar vid införandet av de nya europeiska sanktionsmöjligheterna, eftersom många svenska aktörer inte vant sig vid att behöva förhålla sig till personuppgiftsregler.

Svaghet: bristande möjligheter för enskilda att få rättvisa (kapitel VIII)

Rättsmedel, ansvar och sanktioner regleras i förordningens kapitel VIII och omfattar följande rättigheter och möjligheter: Rätt att lämna in klagomål till en tillsynsmyndighet (artikel 77), rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut (artikel 78), rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde (artikel 79), företrädande av registrerade (artikel 80), vilandeförklaring av förfaranden (artikel 81), ansvar och rätt till ersättning (artikel 82), allmänna villkor för påförande av administrativa sanktionsavgifter (artikel 83), sanktioner (artikel 84).

De höga sanktionerna i dataskyddsförordningen (upp till 4% av den globala årsomsättningen för ett företag) gäller inte enskildas rätt att utkräva ansvar av leverantörer eller myndigheter som klantat sig eller brutit mot lagen, utan är en rätt för ansvarig tillsynsmyndighet (i Sverige Datainspektionen) att utkräva sanktionsavgifter.

Dataskyddsförordningens artiklar 83(4) och 83(5) innehåller maxtak för sanktionsavgifter, vilket är ett sätt att skydda särskilt stora företag från att drabbas av de största sanktionerna. Ett företag globala vars årsomsättning är högre än 500'000'000 euro per år lider mindre risk av att bryta mot dataskyddsförordningens bestämmelser än ett företag vars globala årsomsättning är mindre än 500'000'000 euro. Det kan anses vara en brist i förordningen eftersom stora företag får en fördel gentemot små företag. Det är dock svårt att se hur någon svensk politisk insats skulle kunna åtgärda denna omständighet i dagsläget.

I artikel 83(7) finns en möjlighet att undanta myndigheter från administrativa sanktionsavgifter. Denna bör inte realiseras i Sverige.

Förslag: Den ekonomiska styrningen av myndigheterna från Ekonomistyrningsverket sådan att det kan vara svårt för myndigheterna att motivera ett gediget dataskydds- och datassäkerhetsarbete om det inte finns ekonomiska konsekvenser av att låta bli att ha ett gediget sådant arbete. Detta märks inte minst på Riksrevisionens återkommande kritik mot myndigheternas IT-säkerhetsarbete.[4] Om risken för administrativa sanktionsavgifter gjordes reell, skulle detta kunna faktoriseras in i myndigheternas budgetar utan att Ekonomistyrningsverket kan uppfatta pengaallokeringen som flådig. Det kan i sin tur höja både dataskydd och IT-säkerhet i myndigheternass verksamhet.

[4] Riksrevisionen (20 november 2014) "Informationssäkerheten i den civila statsförvaltningen (RiR 2014:23)"; Riksrevisionen (26 maj 2016) "Informationssäkerhetsarbete på nio myndigheter (RiR 2016:8)"; Riksrevisionen (2007) "Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen (RiR 2007:10)"

Svaghet: Effektiva rättsmedel

Angående definitionen av effektiva rättsmedel i artikel 78 och 79 dataskyddsförordningen finns inom svensk kontext särskilda brister. Utredningsdirektiven Dir. 2016:15 begränsar omfattningen av begreppet "effektiv" till överklagans-

möjlighet.[25] I Europarådets rådgivande dokument för effektiva rättsmedel ingår dock att rättsmedlena ska vara tillgängliga och innebära tillräckliga sanktioner för att beivra framtida brister.[26] Detta kan mot bakgrund av de atypiskt låga skadeståndsmöjligheterna i Sverige inte antas vara fallet.[27]

Utredningsuppdraget har också uttryckligen begränsat utredaren från att titta närmare på möjligheten för konsumentorganisationer och fristående organisationer att lämna in klagomål å registrerades vägnar utan registrerades föregående samtycke.[28] Det gör det i princip svårare för enskilda att passivt försvara sina intressen genom att gå med i en organisation som verkar för bättre dataskydd (jämför skäl 142 i förordningen). Notera att till exempel Sveriges konsumenter idag kan lämna in klagomål till tillsynsmyndigheter utan att först aktivt mobilisera ett stort antal enskilda. Det vore inte orimligt att samma skyddsteknik används inom dataskyddsområdet.

Till sist saknas i Sverige, till skillnad från i till exempel USA, en tradition av grupptalan trots att de flesta dataskyddsinskränkningar drabbar många enskilda samtidigt.

Regeringens minimalistiska tolkning av dataskyddsförordningens bestämmelser kring rätt för enskilda att utöva sina rättigheter, innebär en begränsning av enskildas möjligheter att utöva sina rättigheter. Bättre möjligheter för enskilda att representeras i kombination med bättre möjligheter till högre skadestånd skulle kunna bli en del av ett effektivt rättsskydd för enskilda.

Källor

- Amberhawk Training (4 maj 2016) ”How ’flexible’ can the UK actually be on EU data protection law?”, The Register. http://www.theregister.co.uk/2016/05/04/will_the_uks_approach_to_the_gdpr_be_harmonised/
- Artikel 29-gruppen, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf
- California Senate. Bill number: SB 1386, An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. 12 februari, 2002. http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
- Chris Chambers (1 juli 2014) ”Facebook fiasco: was Cornell’s study of ‘emotional contagion’ an ethics breach?”, The Guardian. https://www.theguardian.com/science/head-quarters/2014/jul/01/facebook-cornell-study-emotional-contagion-ethics-breach
- Council of Europe, Guide to Good Practise in Respect of Domestic Remedies. http://www.echr.coe.int/Documents/Pub_coe_domestics_remedies_ENG.pdf
- Datainspektionen (8 juni 2016) ”Vårdgivare måste förhindra att anställda får för vid åtkomst till journaluppgifter” http://www.datainspektionen.se/press/nyheter/2016/vardgivare-maste-forhindra-att-anstallda-far-for-vid-atkomst-till-journaluppgifter/
- Datainspektionen (26 oktober 2015) ”Allvarlig kritik mot bristfällig utredning på e-hälsoområdet” http://www.datainspektionen.se/press/nyheter/2015/allvarlig-kritik-mot-bristfallig-utredning-pa-e-halsoomradet/
- Datainspektionen (8 juli 2015) ”Tydligare information krävs vid forskningsstudier” www.datainspektionen.se/press/nyheter/2015/tydligare-information-kravs-vid-forskningsstudier/

[25] s. 11 Dir. 2016:15 Dataskyddsförordningen.
[26] Council of Europe, Guide to Good Practise in Respect of Domestic Remedies.
[27] Se ovan fotnot 24.
[28] s 12 Dir. 2016:15 Dataskyddsförordningen.

- Datainspektionen (27 april 2015) ”Tillfällig forskningslag bör inte förlängas” http://www.datainspektionen.se/press/nyheter/2015/tillfallig-forskningslag-bor-inte-forlangas/
- Datainspektionen (12 februari 2015) ”Kritik mot lagförslag för registerbaserad forskning” http://www.datainspektionen.se/press/nyheter/2015/kritik-mot-lagforslag-for-registerbaserad-forskning/
- Europeiska unionen, Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:sv:HTML
- Europeiska unionen, Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32002L0058&qid=1465563881371&from=EN
- Europeiska unionen, 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
- Europeiska unionen, Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:sv:PDF
- Europeiska unionen, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Europeiska unionen, RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Europeiska unionen, VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Fundamental Rights Agency, Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), komparativ studie, maj 2010. Se särskilt s. 43. Tillgänglig på: http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities
- Fundamental Rights Agency, Access to data protection remedies in EU Member States, januari 2014. Se s. 21 i rapporten. Tillgänglig på: http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states
- Kommittédirektiv 2014:164 En myndighet med ett samlat ansvar för tillsyn över den personliga integriteten http://www.regeringen.se/rattsdokument/kommittedirektiv/2014/12/dir.-2014164/
- Kommittédirektiv 2016:15 Dataskyddsförordningen http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/02/dir.-201615/
- Kommittédirektiv 2016:41 En ändamålsenlig reglering för biobanker http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/05/dir.-201641/
- Myndigheten för samhällsskydd och beredskap, Obligatorisk it-incidentrapportering. https://www.msb.se/sv/Forebyggande/Informationssakerhet/It-incidentrapportering/

- Riksrevisionen (2007) ”Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen (RiR 2007:10)” http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2007/Regeringens-styrning-av-informationssakerhetsa i-den-statliga-forvaltningen-/
- Riksrevisionen (20 november 2014) ”Stora brister i statens arbete med informationssäkerhet” http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2014/Informationssakerheten-i-den-civila-statsforvaltningen/
- Riksrevisionen (26 maj 2016) ”Informationssäkerhetsarbete på nio myndigheter (RiR 2016:8)” http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2016/Informationssakerhetsarbete-pa-nio-myndigheter/
- Sasha Romanosky, David Hoffman, Alessandro Acquisti ”Empirical Analysis of Data Breach Litigation” i WEIS 2010: http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf
- Scott Berinato (12 februari 2008) ”CSO Disclosure Series | Data Breach Notification Laws, State By State”, CSO-ONLINE. http://www.csoonline.com/article/2122493/compliance/cso-disclosure-series---data-breach-notification-laws--state-by-state.html
- SOU 2012:90 Överskottsinformation vid direktåtkomst http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/01/sou-201290/
- SOU 2015:39 Myndighetsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/
- SOU 2016:7 Integritet och straffskydd. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/02/sou-20167/
- SOU 2016:41 Hur står det till med den personliga integriteten? - en kartläggning av Integritetskommittéen http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/06/sou-201641/

Vita huset, ”We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consu- mers Online”, 23 februari 2012. https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

Övriga svagheter i dataskyddsförordningen

Svaghet: information till den registrerade om en personuppgiftsincident (artikel 34)

Incidentrapportering har de senaste två åren fått stort utrymme även i den svenska debatten. Just nu finns inte mindre än fyra separata initiativ, den allmänna dataskyddsförordningen inkluderat, för incidentrapportering. Grunden för incidentrapportering kommer från amerikansk lagstiftning, där delstaten Kalifornien 2002 införde en skyldighet för företag att rapportera till invånare i Kalifornien då deras hälso- eller finansuppgifter riskerat att hamna i otillbörliga händer.[29] Den kalifornska lagstiftaren har sedan spritt sig till många andra delstater.[30] I USA innebär rätten att bli informerad en rätt att ställa leverantören till svars för dess handlingar. Varje enskild individ vars uppgifter otillbörligen spritts har genom incidentrapporteringslagstiftningen en möjlighet att utkräva ansvar av leverantörer som inte vidtagit tillräckliga säkerhetsåtgärder mot olovlig spridning.[31]

[29] California Senate. Bill number: SB 1386, An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. 12 februari, 2002.

[30] Scott Berinato (12 februari 2008) ”CSO Disclosure Series | Data Breach Notification Laws, State By State”, CSO-ONLINE.

[31] Sasha Romanosky, David Hoffman, Alessandro Acquisti. ”Empirical Analysis of Data Breach Litigation” i WEIS 2012.

De europeiska incidentrapporteringsbestämmelserna har ett annat fokus. I Sverige har man framför allt fokuserat på Myndigheten för samhällsskydd och beredskaps möjligheter att tillverka statistik över inträffade incidenter.[32] Lagstiftningen om incidentrapporter för tillhandahållare av elektroniska kommunikationsnät i EU:s förordning ger Post- och telestyrelsen möjlighet att inleda tillsyn,[33] men innebär inga avsevärt förbättrade möjligheter för enskilda att hålla leverantörer ansvariga för säkerhetsfel.[34] Det europeiska nätverks- och informationssäkerhetsdirektivet[35] har återigen ett fokus på en tillsynsmyndighets möjligheter att bilda sig en statistisk uppfattning om vilken sorts incidenter som äger rum, snarare än möjligheter för individer att utkräva ansvar för inträffade incidenter.

Även i dataskyddsförordningen finns begränsningar på de omständigheter då individer ska informeras. Ett inträffat säkerhetsproblem ska ”sannolikt leda till hög risk för fysiska personers rättigheter” innan en enskild behöver informeras om det inträffade problemet.

Begreppen ”sannolikt” och ”hög risk” kommer att tolkas av Datainspektionen och andra europeiska tillsynsmyndigheter. Det finns i princip inget som förhindrar att de tolkar bestämmelsen på ett sådant sätt att EU:s allmänna dataskyddsförordning utsträcker liknande rättigheter till europeiska konsumenter som amerikanska konsumenter redan har. Tillsynsmyndigheternas självständighet begränsar dock det politiska handlingsutrymmet att formellt styra deras tolkning av enskildas rättigheter enligt artikel 34.

Svaghet: Prioriteringsordningen mellan företags immateriella rättigheter och enskildas rätt till dataskydd (skäl 63, artikel 13(2)(f), artikel 20(4))

Under dataskyddsdirektivet 1995 hade individer en rättighet att få reda på den logik som ligger bakom automatiska beslut.[36] Detta kunde tolkas som en möjlighet att få reda på hur de algoritmer är utformade som på bas av personuppgifter avgör hur en individ ska behandlas. I praktiken kunde denna rättighet inte användas, eftersom lagstiftaren hade infört ett absolut krav på att rätten att få reda på logiken bakom automatiska beslut inte skulle inskränka företags immateriella rättigheter, så som företagshemligheter och upphovsrätter i mjukvara.[37]

I förordningen är detta krav uppluckrat (skäl 63) och rätten att få reda på logiken är skärpt (artikel 13(2)(f)). I den allmänna dataskyddsförordningen lämnas det öppet för en intresseavvägning mellan företagens rättigheter att hålla infor-

[32] Myndigheten för samhällsskydd och beredskap, Obligatorisk it-incidentrapportering.

[33] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) samt Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation.

[34] Post- och telestyrelsen inledde 2014 en tillsyn av kundplacerad teknisk utrustning, efter att Dagens nyheter hade rapporterat att det var enkelt att utnyttja säkerhetsfel i hushållsroutrar. Tillsynen avslutades 2015 utan vidare åtgärder med observationen att teleoperatörerna hade åtagit sig att publicera mer konsumentinformation på sina hemsidor.

[35] Direktivet verkar ännu inte vara publicerat i EU:s officiella tidskrift för lagstiftning, men lite information finns här: http://www.consilium.europa.eu/en/policies/cyber-security/

[36] Artikel 12(a), Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

[37] Skäl 41, Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

mation hemlig, och individers möjligheter att få reda på hur de påverkas. Detta kan öppna upp för mer oberoende forskning kring algoritmisk reglering. Idag är forskning på algoritmer och deras konsekvenser i princip begränsad till forskare med anknytning till företag som använder sig av algoritmiskt beslutsfattande.[38]

I artikel 20(4) dataskyddsförordningen har lagstiftaren gjort en avvikelse från principen om större öppenhet, och istället dikterat att företags rättigheter alltid ska anses mer viktiga än individers rättigheter att få nyttjanderätt till information om dem själva. Artikel 20 syftar till att göra det enklare för konsumenter att byta mellan olika tjänster, och man kan tycka det är lite tråkigt att lagstiftaren så uppenbart valt att nedprioritera enskildas rättigheter och möjligheter att utöva desamma.

Det kommer att åligga domstolarna att lösa hur de här artiklarna ska tolkas och vilken konsekvens de får. Enskildas möjligheter att försvara sin rätt att till information kommer vara betydligt svagare än näringslivets parters möjligheter att försvara sin rätt att inte berätta, särskilt då regeringen i Sverige (och sannolikt även andra EU-länder) kan tänkas inskränka möjligheterna för enskilda att bli representerade av organisationer som driver frågor av ett mer principiellt slag (se ovan).

Svårighet: Barns rätt att samtycka (artikel 8(1))

I artikel 8(1) finns särskilda bestämmelser om barns samtycke enligt artikel 6(1)(a) som ådragit sig uppmärksamhet i Sverige. Problemet för tjänsteleverantörer i nätmiljöer med avseende på den juridiska basen ”samtycke” är att de oftast inte åtar sig att göra något för sina ”konsumenter”. När ett barn går med i ett socialt nätverk så som Facebook eller Twitter åtar sig tjänsteleverantören oftast bara en skyldighet att tillhandahålla en odefinierad ”tjänst”. Eftersom ”tjänstens” natur inte framgår i avtalet kan man inte säga att tillhandahållandet av tjänsten kräver någon särskild personuppgiftsbehandling – leverantören åtar sig så att säga inte att levererera reklam till barnet, och barnet skriver inte heller under avtalet för att erhålla reklam. Dessa leverantörer kan alltså inte hänvisa till uppfyllande av avtal (artikel 6(1)(b)) när de behandlar barns personuppgifter.

Vad kravet i artikel 8(1) innebär är att det blir svårare för plattformar som Facebook, Twitter, och Google att behandla barns personuppgifter i marknadsföringssammanhang. Detta är givetvis en stor utmaning för globala plattformar vars främsta intäktskälla är just storskalig profilering och behandling av personuppgifter för marknadsföringssyfte. Samtidigt kan plattformarna tänkas åberopa den juridiska basen i artikel 6(1)(f) (berättigat intresse) istället. Då kommer det landa på tillsynsmyndigheterna att bedöma i vilken utsträckning det är korrekt, rättvist och lagligt att profilera barn.

De flesta medlemsländer, och även USA, har redan en etablerad praxis för hur man får sluta avtal med barn. Till exempel får barn i alla länder och alla åldrar erlägga engångsbetalningar i utbyte mot en vara, jämför inköp av glasstrutar. Däremot är det inte tydligt att barn i alla åldrar får ingå avtal om prenumerationer utan målsmans tillåtelse.

På grund av amerikanska regler för skydd av barn (som kan återfinnas i den amerikanska så kallade COPPA-lagstiftningen) är det vanligt att sociala nätverk

[38] Chris Chambers (1 juli 2014) ”Facebook fiasco: was Cornell’s study of ‘emotional contagion’ an ethics breach?”, The Guardian.

som Twitter och Facebook avkräver sina användare ett löfte om att de är över 13 år. I praktiken ljuger många yngre användare om sin ålder så att de kan gå med i nätverken även om de är yngre än 13 år. De nya europeiska reglerna kommer inte att påverka detta i någon betydande omfattning eftersom de amerikanska reglerna redan skapat det här beteendet bland europeiska ungdomar.

Ett ytterligare problem för barn är att deras målsmän alltid kan samtycka i deras ställe. Det gör att föräldrar kan sprida stora mängder privat information om sina barn (till exempel bilder på barnens fysiska eller beskrivningar av deras mentala utveckling) som sedan kan användas som grund för profilering och marknadsföring utan att barnen egentligen har några möjligheter att säga emot. Rätten att bli bortglömd (artikel 17) kanske i viss utsträckning kan hjälpa barn som blivit tillräckligt gamla för att själva bestämma åtgärda vissa aspekter av sådant föräldrabeteende, men det återstår att se om och hur det är en realistisk åtgärd för barn att begagna sig av.

Oavsett vad som står i lagen kommer barn vara fortsatt beroende av att vuxna personer tar ansvar och beter sig rättvist. Om rätten till privatliv och dataskydd tolkas som en rätt till egen, självständig identitetsutveckling (jämför Seda Gürses) är det uppenbart att barns rätt till självständig identitetsutveckling redan begränsas av att barn är beroende av vuxna i sin omgivning. Vad som är en ”omgivning” till barnet har i sin tur kraftigt expanderats i och med nya och bättre kommunikationsmöjligheter. Sannolikt kommer inte dataskyddslagstiftningen vara tillräcklig för att skydda barn från sådan diskriminering eller särbehandling som kan uppstå till följd av personuppgiftsbehandling.

Observation: Barns rätt till samtycke kommer framför allt att aktualiseras i förhållande till nättjänster som idag har profilering och marknadsföring som främsta intäktskälla. Det kommer i princip att vara upp till tillsynsmyndigheterna hur de applicerar och tillser bestämmelsen.