Stockholm, 16 November 2016

Till Justitiedepartementet

Sig Security har fått tillfälle att avge remissvar över Integritetskommitténs delbetänkande Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén (SOU 2016:41) och får härmed inkomma med följande.

Sammanfattande synpunkter

Sig Security delar i allt väsentligt Integritetskommitténs bedömning och slutsatser. Det är bara att instämma i att hoten mot den personliga integriteten ökar och att de kommer både från myndigheter och enskilda rättssubjekt. Teknikutvecklingen och internationaliseringen är faktorer som på olika sätt bidrar till att öka hotbilden.

Sig Security vill särskilt uppmärksamma om den stora betydelsen åtgärder för informationssäkerhet, IT-säkerhet och säkerhet har för den personliga integriteten. Säkerhetsfrågorna och integritetsfrågorna går hand i hand. Därför är olika slags säkerhetsåtgärder, tekniska, administrativa och organisatoriska särskilt viktiga för att kunna bibehålla och stärka skyddet för den personliga integriteten. I detta ingår att åstadkomma ett bra skydd mot intrång, obehörig åtkomst eller spridning av information eller att informationen används för obehöriga ändamål. Däri ingår även att kunna upptäcka, utreda och beivra sådana obehöriga åtgärder. Sig Security vill därför framhålla informationssäkerheten som ett viktigt verktyg för att stärka den personliga integriteten.

På grund av hur informationstekniken är utformad och uppbyggd, hur tjänsterna på det informationstekniska området organiseras och tillhandahålles i kombination med att detta ständigt förändras och utvecklas, blir det omöjligt för den enskilde att kunna ha koll på vem som har tillgång till information om denne, hur tillgången sker och varifrån informationen åtkommes. Därför anser Sig Security att det är särskilt viktigt att lagstiftning och rättstillämpning anger distinkta gränser för hur informationen får hanteras. Den enskilde måste kunna förutse hur hans eller hennes personuppgifter kan komma att behandlas, vem som kan komma att behandla uppgifterna och för vilka ändamål uppgifterna ska få behandlas.

Den personliga integriteten ställs ibland mot andra viktiga intressen såsom samhällets intresse att kunna behandla uppgifter för att skydda allmänheten och nationell säkerhet. Svårigheten i att hitta en konkret, tydlig och allmängiltig definition av begreppet personlig integritet vållar särskilda problem när den ska vägas mot sådana andra intressen som också är angelägna. Sig Security finner det angeläget att denna problematik uppmärksammas, så att det kan undvikas att integritetsfrågan undervärderas när den jämförs med andra mer konkretiserade och mätbara skyddsintressen.

Sig Security anser det särskilt angeläget att försöka bedöma vilka tänkbara effekter eller konsekvenser intrång i den personliga integriteten kan leda till. Förutom den skada eller olägenhet som den enskilde kan åsamkas, kan sådana intrång även leda till att allmänheten tappar förtroendet för informationstekniken och blir tveksam till användandet av denna vilket inte ligger i samhällets intresse. Att försöka sätta sig in i vilka olika skador och olägenheter som kan uppstå blir därför en fortsatt viktig uppgift. Sig Security vill därför framhålla informationssäkerheten som ett viktigt redskap för att förhindra intrång i den personliga integriteten.

Det kan inte helt undvikas att intrång i den personliga integriteten kommer att uppstå. Det beror på att ingen teknisk lösning eller hanteringen därav är hundraprocentigt säker. Därtill kommer det att finnas sådana intrång som måste kunna anses behöriga även i ett öppet demokratiskt samhälle som vårt. Sig Security ser det som angeläget att närmare kartlägga vilka slags olägenheter som skulle kunna drabba de enskilda och hur olägenheterna kan undvikas eller på vilket sätt de drabbade kan kompenseras. Felaktiga eller missvisande uppgifter om de enskilda skulle kunna leda till avsevärda olägenheter för dem. En särskild svårighet i detta sammanhang och som förtjänar att uppmärksammas är att de enskilda inte alltid får kännedom om vilka uppgifter som behandlas eller ens att de behandlas. Även om Sig Security kan instämma i det mesta av Integritetskommitténs analyser skulle det ha varit välkommet med mera konkreta förslag om hur bristerna ska kunna åtgärdas, t.ex. genom skärpt lagstiftning. Sig Security anser det även vara önskvärt med en mer ingående analys av vilka tänkbara konkreta konsekvenser som kan uppstå till följd av de olika omnämnda exemplen på intrång i den personliga integriteten.[1]

Integritetskommittén uttrycker en oro för de stegvisa försämringarna av skyddet för den personliga integriteten, vilket är en oro som Sig Security instämmer i. Denna oro bör föranleda vissa mycket relevanta frågeställningar t.ex. kring var gränsen går för hur långt denna försämring får fortsätta eller vad vi kan göra för att öka den enskildes möjligheter att kunna kontrollera hur dennes uppgifter behandlas.[2]

Därutöver får Sig Security anföra följande.

Författningsförslagen

Sig Security noterar att Integritetskommittén har ett enda förslag till författningsändring, nämligen till förordning om ändring av förordningen (2007:975) med instruktion för Datainspektionen.[3] Förslaget innebär att Datainspektionen årligen ska rapportera till regeringen om situationen för integritetsskyddet. SIG Security ställer sig bakom förslaget eftersom detta sätter ökat fokus på integritetsfrågorna men samtidigt även på informationssäkerheten. Det bör samtidigt uppmärksammas om att Datainspektionen kommer att få ett utökat ansvar till följd av att Europeiska unionens Allmänna dataskyddsförordning ska börja tillämpas den 25 maj 2018. SIG Security känner oro för att Datainspektionen i nuläget inte har tillräckligt med resurser för att uppfylla det ökade ansvar och de ytterligare arbetsuppgifter som detta för med sig. Sig Security anser dessa förhållanden föranleda att ökade resurser ställs till Datainspektionens förfogande.

[1] Jfr SOU 2016:41 s. 27 ff.
[2] Jfr SOU 2016:41 s. 33
[3] SOU 2016:41 s. 35

Vad är personlig integritet?

Sig Security delar Integritetskommitténs uppfattning att vad som ska anses utgöra personlig integritet inte är definierat och kan uppfattas olika utifrån olika förutsättningar och i olika sammanhang. Den personliga integriteten kan knappast uttryckas som en parameter av visst värde när den ska vägas mot annan parameter som t.ex. samhällsnyttan eller företagsnyttan som i högre grad låter sig uppmätas i form av sparade kostnader, uppnådda resultat eller ekonomisk vinst.

Motsvarande resonemang gör sig enligt Sig Securitys uppfattning gällande även om den personliga integriteten uttrycks som en ”normal fredad privat sfär”. Även med detta synsätt blir det svårt att uppskatta uttryckets värde.[4]

Bedömning av riskerna för den personliga integriteten

Vad som ska anses utgöra oönskade konsekvenser för den personliga integriteten bör enligt Sig Security även betraktas utifrån vems perspektiv det bedöms om konsekvenserna är oönskade. Vad som är oönskat för den vars personuppgifter behandlas är kanske önskvärt för den som behandlar uppgifterna.

Sig Security anser det vara viktigt att samhället och de enskildas syn på vad som är oönskade konsekvenser så långt som möjligt – helst helt – sammanfaller.[5] Det måste också beaktas att ett mindre intrång i någons personliga integritet kan leda till en betydande skada, samtidigt som ett mer omfattande intrång kan leda till en mindre skada. Sig Security vill därmed framhålla att även de tänkbara konsekvenserna av ett intrång i den personliga integriteten måste vägas in och att bedömningen inte bara kan utgå ifrån uppgiftens art eller varför uppgiften behandlas.[6]

Den samlade effekten för den enskilde

Sig Security instämmer i beskrivningen av hur situationen för den personliga integriteten har utvecklats och får i sammanhanget framhålla att det samtidigt är viktigt att väcka frågan hur långt det kan vara acceptabelt att denna utveckling fortgår och när den når en gräns för vad som är acceptabelt i ett demokratiskt samhälle. Det är önskvärt att det finns en tydlig markering av vilka slags intrång i den personliga integriteten och vilka konsekvenser av sådana intrång som inte är acceptabla.[7]

Kunskapen om hur uppgifterna hanteras

Att enskilda är okunniga om hur och varför deras uppgifter behandlas eller av vem uppgifterna behandlas är i sig illa nog. När myndigheter eller företag kan behandla uppgifter genom att anlita annan för att sköta informationshanteringen, t.ex. genom att använda molntjänster, utan att ha satt sig in i hur dessa fungerar blir det fråga om en okunskap som ytterligare ökar riskerna för den personliga integriteten.[8]

---

[4] SOU 2016:41 s. 39
[5] SOU 2016:41 s. 40
[6] SOU 2016:41 s. 41 f.
[7] SOU 2016:41 s. 50 ff
[8] SOU 2016:41 s. 53

Möjligheten för den enskilde att påverka

En situation där de enskildas okunskap eller bristande möjlighet att förstå hur eller varför deras uppgifter behandlas är när de tillåtna ändamålen för vilka uppgifter får behandlas definieras på ett luddigt och öppet sätt. När det även kan bli fråga om att behandla uppgifterna för olika tillkommande s.k. sekundära ändamål får den enskilde ännu svårare att kunna förutse konsekvenserna av uppgiftsbehandlingen. Många bestämmelser innehåller just sådana primära eller sekundära ändamål som är diffusa, t.ex. som hänvisar till att uppgifter får vidarebefordras till olika andra myndigheter som därefter får behandla dem för sina respektive ändamål som från tid till annan definieras i berörd speciallagstiftning.[9]

Den enskildes egna skyddsåtgärder

Den enskildes kunskap om vilka olika skyddsåtgärder som står till buds är även enligt Sig Securitys uppfattning begränsad. Om endast kriminella kommunicerar på ett skyddat sätt kan det vara frestande för samhället att i stället kontrollera allmänheten för att rikta krav och påföljder mot dem för vissa mindre allvarliga förseelser eller bara för att kontrollera för kontrollens egen skull[10] Därför är det utifrån Sig Securitys erfarenheter och uppfattning viktigt att de enskilda informeras och blir alltmer kunniga om vilka olika slags åtgärder för informationssäkerhet som står till buds och hur de kan användas. Det blir också allt viktigare för leverantörer att göra informationssäkerhetstjänsterna allt enklare och mer lättillgängliga så att allt fler kan använda dem. Samtidigt vill Sig Security framhålla intresset i att kontrollapparaten riktas mot de hot och risker som verkligen förtjänar att kontrolleras, annars kan detta hämma förtroendet för informationstekniken och teknikutvecklingen.

Otillräcklig tillsyn och sanktionerna

Med de resurser som tilldelas tillsynsmyndigheterna finns det enligt Sig Security anledning att oroa sig för att samhällets engagemang för att skydda den personliga integriteten är och förblir ytterst begränsat.

Som Integritetskommittén konstaterar används straff- eller skadeståndssystemet sällan i samband med intrång i den personliga integriteten, vilket tyder på att vi som enskilda knappast kan räkna med någon hjälp från myndigheterna vid olika slags integritetsintrång. När regelverket som Integritetskommittén nämner är oprecist och otydligt torde detta göra det svårt att utkräva något ansvar från de inblandade aktörerna.[11] De skadestånd som utbetalats uppgår oftast inte heller till några särskilt avskräckande belopp. I normalfallet torde det bli fråga om ersättningar uppgående till ca 5 000 – 10 000 kronor.[12] Sig Security anser det därför även av dessa skäl vara önskvärt att det tydliggörs i tillämpliga regelverk gränsen för vad som kan anses vara acceptabla intrång i den personliga integriteten och vilka krav på informationssäkerheten som ska gälla. Samtidigt anser Sig Security att denna problematik även bör föranleda att Datainspektionen tilldelas ytterligare resurser för sitt uppdrag, särskilt inför de ökade krav som följer av Europeiska unionens Allmänna dataskyddsförordning.

[9] SOU 2016:41 s. 53 f
[10] SOU 2016:41 s. 55
[11] SOU 2016:41 s. 56 f
[12] Se t.ex. JK:s beslut 2002-10-15, dnr 1075-02-40 och 2003-09-11, dnr 2081-03-42 och 2974-02-42

Globaliseringen

Sig Security vill fästa uppmärksamhet på att sådana informationstekniska tjänster som innebär att informationshanteringen kan ske utomlands inte bara kan få konsekvenser utifrån den personliga integriteten.

Det kan även ifrågasättas om användandet av sådana tjänster inte rentav kan strida mot tillämpliga regler om sekretess eller tystnadsplikt. När teknik används som innebär att uppgiftshanteringen sker utomlands, t.ex. i samband med användandet av molntjänster eller vid annan outsourcing, innebär detta att myndigheterna eller företagen väljer en teknik som i praktiken innebär att informationen gjorts tillgänglig eller utlämnats till andra länder myndigheter enligt de regelverk som gäller där, detta oberoende av om detta är tillåtet enligt svensk lag.[13]

Personlig integritet ett viktigt värde för hela samhället

Sig Security ställer sig bakom att den personliga integriteten är viktigt inte bara för den enskilde själv, utan för samhället i stort. Det ligger i samhällets intresse att informationstekniken utvecklas och används inom allt fler områden i samhällslivet, eftersom detta kan förenkla och effektivisera. Detta förutsätter att allmänheten inte bara kan lita på att informationstekniken faktiskt fungerar på avsett sätt, utan även att den information som förekommer inte används för några olämpliga eller oförutsebara områden. I annat fall riskeras att allmänheten kommer att avstå från att använda tekniken, något som inte ligger i samhällets intresse. Detta ökar i sin tur betydelsen i att inte bara samhället utan även de enskilda engagerar sig i informationssäkerhetsfrågorna.

Om inte integritetsfrågorna och säkerhetsfrågorna ges tillräcklig uppmärksamhet återstår kanske endast alternativet för de enskilda att minimera användandet av informationstekniken om de inte vill riskera oacceptabla kränkningar av den personliga integriteten, t.ex. genom att bli registrerade, kartlagda eller övervakade.[14]

Teknikutvecklingen och kunskapsläget

Utvecklingen på det informationstekniska området är sådant att vi inte kan förutse vilka tjänster, användningsområden eller affärsmodeller som kommer att dyka upp. Detta är i sig en risk som enligt Sig Security borde leda till större eftertanke. Integritetsskyddande teknik är därför ett område som Sig Security finner särskilt intressant utifrån sitt uppdrag och ändamål. Sådan teknik måste vidareutvecklas samtidigt som den måste bli enklare att använda, där enskilda informeras klart och tydligt om vilka säkerhetslösningar som finns och hur de används.[15] Sig Security anser att dessa målsättningar inte kan uppfyllas om inte tekniker, jurister, samhällsvetare, ekonomer och andra samverkar och integreras med varandra för att utarbeta de tekniska lösningarna på ett lämpligt sätt.[16]

---

[13] SOU 2016:41 s. 58, se t.ex. 8 kap. 3 § offentlighets- och sekretesslagen (2009:400)
[14] SOU 2016:41 s. 61
[15] SOU 2016:41 s. 63
[16] SOU 2016:41 s. 64

Drivkrafter bakom utvecklingen

Hur integritets- och säkerhetsfrågorna ska bli ett prioriterat intresse för ledningen hos våra myndigheter och företag är ett problem som Sig Securitys olika medlemmar ställts inför i sitt dagliga arbete. Myndigheter och företag vill naturligtvis effektivisera sitt arbete, spara kostnaderna, öka intäkterna eller på annat sätt framgångsrikt utföra sitt uppdrag. Mot en sådan bakgrund är det inte förvånande att dessa intressen hamnar i blickpunkten hellre än integritetsintresset för den som uppgifterna gäller. Det delas inte ut några prispengar, bonusar eller andra pluspoäng till den som hos myndigheten eller företaget begränsat användningen av uppgifter för att skydda någons personliga integritet.[17]

Kommitténs bedömning av respektive område

Forskning och statistik

När det som Integritetskommittén konstaterat inte finns inte många andra länder som kan jämföra sig med Sverige när det gäller möjligheten för det allmänna att undersöka sina invånares liv, borde detta enligt Sig Security mana till eftertanke. Denna bör leda till frågan om all denna ansamling av personuppgifter verkligen är nödvändig, om alla dessa kontrollmöjligheter verkligen leder till någon nytta, samt för vem uppgifterna i så fall är till nytta – staten eller den enskilde.[18]

Uppgifter i molnet

När Integritetskommittén påtalar olika rättsliga överväganden som blir aktuella i samband med hur myndigheter väljer att hantera sina uppgifter finns det enligt Sig Security särskild anledning till eftertanke. Det inte finns klart rättsligt stöd för att tillgängliggöra eller lämna ut information till externa aktörer som ska sköta infohanteringen åt myndigheter eller andra när informationen omfattas av sekretess eller tystnadsplikt. På vilken grund är tillgängliggörandet eller utlämnandet "behörigt" enligt offentlighets- och sekretesslagen (2009:400) eller andra berörda registerlagar om det inte finns uttryckligt stöd för detta, t.ex. genom en sekretessbrytande regel eller att situationen räknats upp i lagtexten eller förarbetena som exempel på när detta är "behörigt"? En extensiv tolkning av bestämmelser om sekretess eller tystnadsplikt för att möjliggöra molntjänster eller annan outsourcing kan bana väg för att bestämmelserna uppfattas som att de gäller bara när det passar. Då urholkas den personliga integriteten och förtroendet för informationstekniken ytterligare.[19]

Sociala medier och e-post

Sig Security vill i detta sammanhang särskilt uppmärksamma om att villkoren för sociala medier oftast innebär att användaren ger leverantören en fullständig rätt att fritt använda inlagda uppgifter, oberoende av om användaren har rätt att göra det t.ex. enligt personuppgiftslagen (1998:204) eller upphovsrättsliga regler. Okunskap om vad villkoren innebär och vad lagreglerna medger kan försätta användarna i bekymmersamma situationer.[20]

---

[17] SOU 2016:41 s. 65
[18] SOU 2016:41 s. 77
[19] SOU 2016:41 s. 81
[20] SOU 2016:41 s. 89 f.

Försäkringsbolag, banker, kreditupplysnings- och inkassoföretag[21]

Sig Security instämmer i Integritetskommitténs bedömning att det är oklart för den enskilde vad ett samtycke från denne egentligen innebär och medför. I många fall förstärks problematiken av att den enskilde knappast har något egentligt val om han eller hon vill komma i åtnjutande av den produkt eller tjänst det är fråga om. Samtycket lämnas därmed mer eller mindre slentrianmässigt och det kan ifrågasättas om det ens kan anses vara fråga om ett frivilligt samtycke.

Samtidigt får Sig Security framhålla att det även är oklart vilket skydd den enskilde egentligen har av den tystnadsplikt som följer av specialbestämmelser för försäkringsbolag, banker och andra finansieringsinstitut, kreditupplysnings- och inkassoföretag. I dessa bestämmelser anges att uppgifter om den enskilde inte ”obehörigen” får röjas.[22] I förarbetena räknas olika situationer upp när ett röjande kan anses behörigt, varav särskilt kan nämnas samtycke eller när uppgiftsskyldighet följer av lag.[23] Det är inte helt lätt att kunna förutse vilka slags röjanden som kommer att anses ”obehöriga” eller ”behöriga”. Om detta ges en extensiv tolkning och även kan omfatta olika situationer där det är ”praktiskt, lämpligt, ändamålsenligt, rimligt” etc. att få röja uppgiften, då blir det tveksamt och oförutsebart för den enskilde att kunna bedöma vilket skydd hans eller hennes uppgifter egentligen har. Detta gör sig särskilt gällande om det ska bli fråga om att låta någon extern leverantör ombesörja informationshanteringen, t.ex. genom en molntjänst. En sådan lösning förutsätter ju att leverantören får tillgång till uppgifterna och då har de ju utlämnats till denne. Om detta i stället kan anses utgöra ett obehörigt röjande gör sig försäkringsbolagen, bankerna, kreditupplysnings- och inkassoföretagen skyldiga till brott mot tystnadsplikt, något som knappast är i linje med intresset av en ändamålsenlig teknikutveckling. Sig Security anser därför att det är önskvärt med ett förtydligande i lag eller förarbeten där det framgår att det även i sådana situationer kan anses vara fråga om ett behörigt röjande. Samtidigt måste i sådana fall informationssäkerhetsfrågorna ges särskilt stor uppmärksamhet, så att det kan säkerställas att leverantören inte missbrukar uppgifterna och att lämpliga åtgärder – tekniska, organisatoriska och administrativa – vidtas för att garantera tystnadsplikten och säkerheten i samband med användande av molntjänster eller andra former av outsourcing.

Identitetsstölder och identitetskapning

Sig Security finner liksom Integritetskommittén att identitetsstölder och identitetskapningar är ett växande problem. Detta kan ställa till med stora problem, inte bara för de enskilda som drabbas, utan även för samhället, myndigheterna och näringslivet. I förlängningen kan detta leda till att förtroendet för de informationstekniska tjänsterna skadas. Om bankerna och andra aktörer under dessa förhållanden väljer att ställa högre krav på sina kunder att bevisa att de inte slarvat med sina uppgifter, når vi till slut ett läge där kunderna avstår från att använda tekniken. Då riskerar vi att gå miste om de fördelar som tekniken bidrar med. Innan vi ökar kraven på de enskilda krävs därför särskilt noggranna överväganden. Även detta fenomen måste enligt Sig Security föranleda att informationssäkerhetsfrågorna ges särskild uppmärksamhet.[24]

---

[21] SOU 2016:41 s. 91 ff. och 99 f.
[22] Se t.ex. 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse, 14 § kreditupplysningslagen (1973:1173) och 11 § inkassolagen (1974:182)
[23] Se t.ex. prop. 1974:42 s. 102 och 2002/03:39 s. 478 ff.
[24] SOU 2016:41 s. 95

Sättet för utlämnande av uppgifter[25]

Sig Security finner att den faktiska skillnaden mellan vad som kan kallas direktåtkomst respektive utlämnande i elektronisk form blir alltmer otydlig allteftersom tekniken utvecklas. Det kan ifrågasättas om distinktionen egentligen är meningsfull. Direktåtkomst kan anses föreligga vid ett automatiserat utlämnande där den som begär uppgiften själv inhämtar den[26], medan utlämnandet i elektronisk form sker manuellt efter en begäran men med användande av informationstekniska medel. Genom att erbjuda direktåtkomst till uppgifter som i förväg bedömts alltid kunna lämnas ut kan i princip samma resultat uppnås som vid ett utlämnande i elektronisk form i varje enskilt fall, med den skillnaden att det inte längre behövs en manuell handpåläggning från någon personal. Sig Security får även här framhålla informationssäkerheten som ett viktigt redskap för att skapa förutsättningar för ett ökat användande av direktåtkomst till olika uppgifter och att det är önskvärt att lagstiftningen ökar möjligheterna till sådan direktåtkomst.

De brottsbekämpande myndigheternas verksamhet[27]

Tillgång till uppgifter i brottsbekämpningen

Sig Security kan instämma i många av Integritetskommitténs slutsatser, men vill särskilt framhålla att en felaktig behandling av personuppgifter i dessa sammanhang kan leda till förödande konsekvenser för den enskilde, särskilt när denne av sekretesskäl inte ens kan få reda på vilka uppgifter myndigheten har tillgång till och behandlar. Om de aktuella personuppgifterna har fått ett felaktigt eller missvisande innehåll finns det stor risk att detta inte uppmärksammas och att myndigheterna grundar sina slutsatser och åtgärder på ett felaktigt underlag. Därtill kommer den enskilde i praktiken knappast heller att kunna räkna med någon kompensation värd namnet för de olägenheter han eller hon drabbats av eftersom myndigheternas agerande sällan kommer att anses tillräckligt bristfälligt för att vara skadeståndsgrundande. Därmed blir informationssäkerhetsfrågorna av största vikt även i dessa sammanhang och kanske särskilt här, eftersom det är fråga om användande av uppgifter i en myndighetsutövning som kan innefatta olika tvångsåtgärder mot de enskilda. Då är det av största vikt att besluten inte fattas på ett oriktigt eller ofullständigt underlag.

Trafikdatalagring[28]

SIG Security får uppmärksamma om att EU-domstolen förklarat bakomliggande EU:s datalagringsdirektiv[29] ogiltigt.[30] Även om en statlig utredning[31] kommit fram till att de svenska nationella datalagringsreglerna om datalagringsskyldighet ska anses giltiga även om direktivet är ogiltigt, anser Sig Security att det inte är helt klart att en skyldighet att lagra data enligt nationella regler ens kan vara möjlig när direktivet ogiltigförklarats.

---

[25] SOU 2016:41 s. 99
[26] Se t.ex. 2 kap. 27-28 §§ lagen (2001:184) om behandling av uppgifter i kronofogdemyndighetens verksamhet
[27] SOU 2016:41 s. 100 ff.
[28] SOU 2016:41 s. 102
[29] EG:s direktiv (2006/24/EG) om lagring av trafikuppgifter
[30] EU-domstolens dom den 8 april 2014 i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., angående giltigheten av datalagringsdirektivet med anledning av begäran av förhandsavgöranden från nationella domstolar i Irland respektive Österrike
[31] SOU 2015:31 – Datalagring och integritet, där slutsatsen blir att svenska nationella regler om datalagring är tillåtna även om datalagringsdirektivet ogiltigförklarats

Om lagstiftningsmakten i detta sammanhang faller under EU:s kompetens torde det inte kunna förekomma nationell lagstiftning på området utan att det säkerställts att denna är förenlig med EU-rätten, såväl formellt som rent innehållsmässigt. Det kan också anses betänkligt utifrån proportionalitetsprincipen att en så stor mängd data lagras som det är fråga om och som potentiellt kan användas för mycket ingående kartläggning av enskilda, när det är så förhållandevis få fall där uppgifterna kommer till nytta. Uppgifternas natur och sammanhang gör att det kan bli förödande konsekvenser för den enskilde om de lagrade trafikuppgifterna är felaktiga eller missvisande. Detta ställer inte bara krav på att de brottsbekämpande myndigheternas behandling av uppgifterna sker korrekt och där uppgifternas tillförlitlighet säkerställts. Det ställer även motsvarande krav på de trafikdatalagrande operatörerna att säkerställa att de aktuella näten och tjänsterna för elektronisk kommunikation är tillfredsställande ur informationssäkerhetsaspekt.[32] Således får Sig Security även i detta sammanhang framhålla att informationssäkerheten är väsentlig för att trafikdata som lagrats och ska användas i brottsbekämpande verksamhet verkligen ska kunna anses tillförlitlig.

Underrättelseverksamheten[33]

Sig Security känner oro för att myndigheter som inte följer gällande bestämmelser för informationshanteringen sällan drabbas av några sanktioner och ifrågasätter därför regelverkets avhållande verkan. Det kan därför vara lämpligt att göra en översyn avseende hur enskilda kan kompenseras och hur myndigheterna effektivare kan avhållas från felaktigheter i sin informationshantering.

Vad gäller information som används för utbyte i underrättelseverksamhet finns det inte några garantier eller ansvar för hur informationen senare används. När det gäller försvarsunderrättelseverksamheten blir försvarssekretessen och därmed naturligt följande hemlighetsmakeri enligt Sig Security ett särskilt problem. Sekretessen gör att det blir särskilt svårt för den enskilde att bedöma vilka uppgifter som behandlas och få dem korrigerade.[34]

Dessa risker förefaller enligt Sig Securitys uppfattning ha underskattats. Samtidigt ser Sig Security en risk för att systemet med underrättelse eller tillsyn från Statens Inspektion för Försvarsunderrättelseverksamheten (SIUN) eller Säkerhets- och integritetsskyddsnämnden (SIN) överskattats och att det kan finns många situationer där den enskilde inte får tillräcklig kännedom om hanteringen av dennes personuppgifter eller förstår hur han eller hon ska agera för att tillvarata sin rätt.[35]

Övervakning med kamera[36]

Sig Security får framhålla att kameraövervakning inte bara kan användas för att övervaka enskilda, utan att det genom sådan övervakning även kan åstadkommas att de enskilda kan skydda sig mot integritetsintrång, t.ex. genom att filma obehöriga ingrepp från myndigheter eller andra enskilda. Det är därför viktigt att tillståndsprövningen inte kantrar så att myndigheter och företag på omotiverade grunder lättare får tillstånd än enskilda.

---

[32] Jfr. 6 kap. lagen (2003:389) om elektronisk kommunikation
[33] SOU 2016:41 s. 102 ff. och 105 ff.
[34] SOU 2016:41 s. 106 ff.
[35] SOU 2016:41 s. 102 f.
[36] SOU 2016:41 s. 108 ff.

Högsta förvaltningsdomstolen (HFD) har nyligen meddelat två domar som angår användandet av övervakningskameror. HFD har kommit fram till att enskildas användande av dashcams eller vindrutekameror anses tillåtna utan krav på tillstånd från Länsstyrelsen[37], eftersom de befinner sig i användarens omedelbara närhet och därför inte är fjärrstyrda.[38] Däremot ansåg HFD att drönare med kameror kräver tillstånd eftersom de manövreras på avstånd.[39]

Molntjänster[40]

Sig Security delar Integritetskommitténs oro för att användandet av molntjänster kan leda till att uppgifter hamnar i länder där lagstiftningen ger ett otillräckligt skydd och där de kan komma att behandlas för ändamål som inte är lagliga i Sverige eller annat EES-land.

Dock har det avgörande från en amerikansk distriktsdomstol angående Microsofts skyldighet att för amerikanska myndigheter förete begärd information även i de fall informationen behandlas i annat land (i detta fall Irland) och som Integritetskommittén hänvisar till[41] överprövats och undanröjts.[42] Rättsläget i USA förefaller därför numera vara att amerikanska myndigheter inte kan runda andra länders regelverk genom att begära in uppgifterna från bolag eller andra rättssubjekt som finns i USA.

Sig Security vill särskilt framhålla att myndigheternas anlitande av externa leverantörer för sin informationshantering inte omfattas av något undantag från sekretessbestämmelserna. Leverantörerna kan inte rakt av anses ingå i myndighetens verksamhet.[43] Inte heller omfattas situationen av någon sekretessbrytande grund.[44] Det kan knappast heller göras en sådan sekretessprövning eller menbedömning som utmynnar i slutsatsen att uppgifter som annars omfattas av sekretess rakt av och generellt kan göras tillgängliga för eller lämnas ut till aktörerna. Detta torde gälla särskilt när sekretessen är absolut, t.ex. vid pågående upphandling, eller omfattas av omvänt skaderekvisit, t.ex. inom hälso- och sjukvården.[45] Motsvarande problematik gäller för olika privata aktörer, t.ex. till följd av banksekretessen och tystnadsplikten för inkasso- och kreditupplysningsföretag där ett röjande inte får ske "obehörigen". I dessa sammanhang finns det inte något uttryckligt stöd vare sig i lagtext eller förarbeten för att ett tillgängliggörande eller ett utlämnande till en extern leverantör som ska sköta infohanteringen per definition kan anses behörigt.[46]

Big Data[47]

Sig Security kan bara instämma i Integritetskommitténs oro över svårigheterna att överblicka vilka uppgifter som kan åtkommas genom Big Data, hur och för vilka ändamål uppgifterna

[37] Se 3, 8 och 9 §§ kameraövervakningslagen (2013:460)
[38] HFD 4110-15
[39] HFD 78-16
[40] SOU 2016:41 s. 111 ff.
[41] Se avgörandet den 31 juli 2014 av Chief U.S. District Judge Loretta A. Preska vid United States District Court, Southern District of New York
[42] United States Court of Appeals for the second circuit, Docket No. 14-2985
[43] Se 2 kap. 1 § offentlighets- och sekretesslagen (2009:400)
[44] Se 10 kap. 2 § offentlighets- och sekretesslagen (2009:400)
[45] Jfr. JO 2011-3032
[46] SOU 2016:41 s. 111 f.
[47] SOU 2016:41 s. 114 f.

kommer att kunna användas, vad som kan komma att ingå i en kartläggning där sådana uppgifter inhämtats är sådana risker som särskilt måste bedömas. I dessa sammanhang blir det enligt Sig Securitys uppfattning särskilt svårt att motverka att informationen används för obehöriga ändamål, blir missvisande eller leder till fel slutsatser.

Biometri[48]

Sig Security vill här framhålla riskerna för att biometriska uppgifter feltolkas och leder till felaktig registrering om en persons egenskaper som sedan kan få oönskade konsekvenser. Denna risk måste uppmärksammas tydligare.

Avslutande synpunkter

Sig Security finner Integritetskommitténs bedömningar och slutsatser välgrundade och alltigenom korrekta. Dock hade Sig Security gärna sett att informationssäkerhetsfrågorna getts större uppmärksamhet. Det kan inte nog framhållas hur nära sambandet är mellan skyddet för den personliga integriteten och de åtgärder – tekniska, organisatoriska eller administrativa – som vidtas för att åstadkomma informationssäkerhet. Det finns även vissa hot mot den personliga integriteten som Sig Security anser hade behövt uppmärksammas ytterligare. Dessutom finns det anledning att överväga ytterligare lagstiftningsåtgärder än dem som Integritetskommittén föreslagit.

Sammantaget välkomnar Sig Security Integritetskommitténs bedömningar och slutsatser och ställer sig bakom dessa.

SIG SECURITY

[48] SOU 2016:41 s. 115 f.