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

DFRI
Föreningen för digitala fri- och rättigheter
ORG.NR 802461-0852 – HTTPS://WWW.DFRI.SE
– DFRI@DFRI.SE

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

DFRI
Box 3644
103 59 Stockholm

MOTTAGARE: Utredningen om moderna regler om beslag och husrannsakan, Justitiedepartementet, 103 33 Stockholm

Inlaga till Ju 2016:08

Inledning

X

Föreningen för digitala fri- och rättigheter är en ideell organisation med syfte att att främja digitala fri- och rättigheter och verka mot censur och inskränkning av yttrandefrihet och personlig integritet.[1] Dataskydd.net är en ideell organisation med syfte att verka för informerade beslut om lagstiftning och teknologi i enlighet med de grundläggande rättigheterna till dataskydd och personlig integritet.[2] Detta är ett gemensamt bidrag till utredarens arbete att hitta ett modernt ramverk för husrannsakan.

Utredningsuppdraget har en digital karaktär. Utredningen har att ta ställning till nya former av husrannsakan och större befogenheter att vid husrannsakan samla in information. Vi lägger särskild vikt vid konsumenters svaga ställning i elektroniska miljöer och rätten till identitet som en förlängning av rätten till privatliv och dataskydd.

Konsumenter har genom en allt mer komplicerad avtalsrätt och EU-rätten blivit ålagda den juridiska risken för både finansiella transaktioner och sina egna identitetsuppgifter i elektroniska miljöer. I sitt IT-säkerhetsarbete har lagstiftaren underprioriterat konsumenters och enskildas möjlighet till integritet och tillförlitlighet i IT-system.[3]

Även rättspolitik som formellt uppfyller kraven i de olika internationella konventioner som Sverige är bundna av påverkar konsumenters möjligheter att nyttja och företags incitament att utveckla säkra och användarvänliga produkter. Vår mening är att myndigheter inte ska bidra eller riskera bidra till sämre förutsättningar för teknisk säkerhet i IT-system. De bör inte heller skapa negativa incitament för privat sektor att ha en så hög nivå för teknisk säkerhet för individer som är ekonomiskt möjlig. Om lagstiftaren vill försämra möjligheterna för teknisk säkerhet så ska lagstiftaren kompensera konsumenter och enskilda med juridisk säkerhet.

[1] https://www.dfri.se/dfri/stadgar/

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

[3] Axel M. Arnbak. ”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives” doktorsavhandling, Universiteit van Amsterdam, 2015.

I fråga om överskottsinformation och beslag gör vi en distinktion mellan ”det allmännas” och ”allmänhetens” intressen av rätten till integritet. Vi formulerar, i enlighet med den utveckling som har skett i Europa och USA, rätten till integritet som en rätt till identitet och självständig identitetsutveckling. Utifrån denna uppfattning om integritetsbegreppet utvecklar vi krav för hur man ska hantera överskottsinformation, tillstånd för husrannsakan, samt kopiering, lagring och gallring av information som de brottsbekämpande myndigheterna förvärvar eller riskerar att förvärva. Vi kopplar detta till en brist på kontrollmekanismer för myndigheternas verksamhet i elektroniska miljöer.

Dir 2016:20.

Vårt dokument följer följande struktur: begreppsdefinitioner (s. 2), något om kontrollmekanismer för svenska myndigheter i digitala miljöer (s. 3), konsumenträttigheter (s. 4), upphandlingar av digitala verktyg för brottsbekämpning (s. 15), teknisk utveckling och individuell säkerhet (s. 11), överskottsinformation och digitala identiteter (s. 20) samt förslag (s. 23). Texten är skriven för att vara läsbar både av den som saknar föregående teknisk kunskap och den som saknar föregående juridisk kunskap. I avdelningen Källhänvisningar på s. 25 finns samtliga källor organiserade efter typ och i alfabetisk ordning.

Genomgång av viktiga begrepp

Vi gör skillnad mellan teknisk säkerhet och juridisk säkerhet.

Teknisk säkerhet.

”Teknisk säkerhet” innefattar tekniska funktioner: funktioner som kan konstrueras, uppfinnas och omsättas på en marknad. En brist på teknisk säkerhet gör till exempel att man kan utföra kort-skimning (kopiera magnetremsan på ett kreditkort), stjäla inloggningsuppgifter, infektera en privatpersons dator med virus, trojaner, och dylikt.

Juridisk säkerhet.

”Juridisk säkerhet” innefattar konsumentinformation, riskfördelning, produktansvar, och frågeställningar om bevisbörda, till exempel vid tvister om vad ett avtal har sagt eller huruvida en produkt fungerat så som en konsument eller privatperson förväntat sig.

Rättssäkerhet.

Vår förståelse av begreppet ”rättssäkerhet” följer Tormod Otter Johansens och Sebastian Wejedals kartläggning av rättssäkerhetsbegreppet enligt artikel 6 Europakonventionen.[4]

Sanktionerade dataintrång.

Att hacka, begå dataintrång, genomföra hemlig dataavläsning, husrannsakan i en dator, husrannsakan på distans och offensiv IT-säkerhet används omväxlande för att beskriva samma tekniska funktioner, nämligen att man utan lov från innehavaren av en viss elektronisk utrustning bereder sig tillgång till funktioner (så som att ändra, läsa, spela in, ta bort, kopiera, radera eller manipulera data, filer, eller programvaror) på utrustningen. Vi kommer att använda begreppet ”sanktionerade dataintrång” som samlingsterm för samtliga dessa begrepp.

Sårbarhet.

En ”sårbarhet” i ett IT-system, även kallat bugg eller säkerhetshål, är ett säkerhetsfel som gör det möjligt att utnyttja IT-systemet på ett sätt det inte är tänkt (till exempel att någon kommer åt funktioner i systemet olovligen).

Åtgärda en sårbarhet.

Att ”åtgärda en sårbarhet” betyder att man ser till att sårbarheten inte längre kan användas för att bereda tillgång till funktioner olovligen. Det innebär oftast att man skriver om programkoden som används för att styra IT-systemet, men

[4] Tormod Otter Johansen och Sebastian Wejedal, “Mot ett funktionellt domstolsbegrepp – Ett bidrag med anledning av den så kallade Försvarsunderrättelsedomstolen”, SvJT 2016 s. 10 (fotnot 190 i del I) respektive s. 191 (s. 17 i del II).

kan också innebära till exempel att man gör en ny och bättre standard för den bakomliggande utrustningen.

0-day.

”0-day” är ett tekniskt begrepp som beskriver en metod att utnyttja tidigare okända sårbarheter i IT-system, som på grund av att de inte tidigare är kända därför inte heller har åtgärdats. Ordet ”0-day” används också för att beskriva en tidigare okänd metod att utnyttja en tidigare känd sårbarhet, som på grund av att sårbarheten inte uppfattats som säkerhetskritisk kanske inte har åtgärdats.

Metoder för att utnyttja sårbarheter.

”Metoder för att utnyttja sårbarheter” är det svenska begrepp vi kommer att använda för att beskriva det som på engelska kallas ”exploits”. Dessa metoder kan begagna sig av redan kända sårbarheter (vilket är normalfallet), eller tidigare okända sårbarheter (i vilket fall metoden är en ”0-day”).

Vi rekommenderar utredaren att göra åtskillnad mellan sådana sårbarheter och metoder för att utnyttja sårbarheter som privatpersoner och företag har haft en möjlighet att åtgärda, och sådana sårbarheter och metoder för att utnyttja sårbarheter som privatpersoner och företag inte har haft en möjlighet att åtgärda.

Internet är ”vilda västern” för brottsbekämpande myndigheter

Idag framstår det som att de brottsbekämpande myndigheterna antar att det som inte är uttryckligen förbjudet skulle vara tillåtet. Till exempel kan polisen be datorkunniga individer att hacka sig in i någons Facebook-konto,[5] och om polisen inte har fått lagstiftarens stöd för att genomföra en viss sorts myndighetsutövning (till exempel begära ut e-postmeddelanden från Hotmail) kan polisen genom avtal med de företag som är villiga att hjälpa polisen genomföra aktiviteter lagstiftaren inte ansett att polisen har behov av.[6]

Polisen har framträtt i svensk riksmedia med kritik mot företag som inte samarbetar med polisen utanför lagens ramar.[7] Det skapar stor osäkerhet kring vilka spelregler som gäller för olika aktörer i samhället på internet. Effektivt är internet ett ”vilda västern” där brottsbekämpande myndigheter och myndigheter anknutna till verksamheter som arbetar för rikets försvar får göra vad de vill, utan översyn, tillsyn eller insyn. Den transparens som finns uppstår genom transparensrapporter från privat sektor eller genom att en journalist eller medborgare lyckas få informella kontakter med någon inblandad i polisens verksamhet.

Arbetsmetoder för brottsbekämpande myndigheter i Sverige har i ökad utsträckning kommit att inspireras av de amerikanska myndigheternas arbetssätt,[8] vilket man kan anta har att göra med det täta operativa samarbetet mellan våra länder och den höga medvetenheten bland svenska makthavare om vissa omständigheter i USA.[9] Tonvikten vid erfarenhetsutbytena och särskilt de politiska

[5] John Bakke (12 juni 2015). ”Polis ville hacka Facebook” SVT.

[6] Se polisens avtal med Facebook och Microsoft så som utlämnade 29 oktober 2015 samt den 4 november 2015: https://dataskydd.net/sites/default/files/microsoft_a439.283.2015.pdf och https://dataskydd.net/sites/default/files/facebook_a449.454.2015.pdf.

[7] Linus Larsson (28 januari 2015) ”Så spanar polisen på Facebook” Dagens nyheter.

[8] Blåljus.nu (20 oktober 2011) ”Hur skulle svenska polischefer klara möte med ”CompStat”?”; Pierre Halsius, ”Nationella insatsstyrkan - nutid och framtid”, Rapport 399 vid Polisutbildningen vid Umeå universitet; Karin Nygren, ”Problemorienterat polisarbete”, Rapport 472 vid Polisutbildningen vid Umeå universitet; Svenska dagbladet (12 februari 2015) ”Anders Ygeman till terrormöte i USA”.

[9] Tobias Brandel (19 februari 2014) ”USA dominerar skev världsbild i riksdagen” Svenska dagbladet.

beslut som följer av samarbetet ligger dock på vilka befogenheter de amerikanska myndigheterna kan utöva, inte vilka kontrollåtgärder som finns för utövandet av befogenheterna. Utredaren behöver tydligt klargöra relationen mellan befogenheter och kontrollsystem för lagstiftaren.

Den fria bevisprövningen i svenska domstolar gör att det inte spelar lika stor processuell roll hur polisen genomfört sitt arbete. Detta är inte fallet i USA, och de brottsbekämpande myndigheterna i USA har mycket starka skäl att följa de procedurer som lagstiftaren dikterat.

I Sverige är skadeståndsrätten sådan att privatpersoner bara får mycket låg ersättning om deras rättigheter har kränkts av myndigheter. I normalfallet är det inte möjligt att alls få ersättning vid en kränkning.[10] I USA är skadestånden för motsvarande kränkningar mycket höga, och även myndigheter kan bli skadeståndsskyldiga.

I Sverige finns inga möjligheter till enkel konstitutionell prövning av polismetoders laglighet och förenlighet med privatpersoners förväntingar på rättssäkerhet. I USA finns flera stora och välfinansierade organisationer (till exempel EFF[11] och ACLU[12]) som kontinuerligt prövar de brottsbekämpande myndigheternas befogenheter och tillämpningar av befogenheter i domstol mot bakgrund av gällande amerikanska medborgerliga rättigheter.

Det finns för- och nackdelar med respektive system. Effekten av det amerikanska inflytandet över de svenska och europeiska brottsbekämpande myndigheternas arbetsmetoder är dock att Sverige blir ”vilda västern”, då befogenheterna och arbetsmetoderna inte är anpassade till de svenska kontrollsystemen.

Man kan jämföra med hur den tyska konstitutionsdomstolen stramat upp kraven för användning av nya hemliga elektroniska tvångsmedel i Tyskland,[13] allt eftersom den tyska lagstiftaren infört huvudsakligen amerikaniserade brottsbekämpningsmetoder.

Konsumenträtt, husrannsakan och elektroniska marknader

Den här delen av texten är en allmän bakgrund för utredningens uppdrag och handlar om konsumenträttsliga frågeställningar om säkerhet, integritet och konfidentialitet i elektroniska miljöer.

Från svensk doktrin finns en snävare men relaterad genomgång i Lennart Johansson i hans avhandling Banker och internet från 2006.[14] Han går igenom hur risken flyttats från banken till konsumenten via avtalsrättsliga konstruktioner. I utländsk doktrin är behandlingen av området mer utförlig:

Teknikhistorikern Jean-Francoise Blanchette[15] gör i sin bok ”Burdens of Proof” en genomgång av juridikens förhållningssätt till kryptografiska (elektroniska) signaturer från och med 1990-talets början. Han beskriver hur lagstiftare har brottats med det komplexa förhållandet vid bestämning av bevisbörda att elektroniska transaktioner ofta innefattar mer än två parter: istället för att ha

[10] Blåljus.nu (30 juni 2015) ”Framtidens polis i förorten”.

[11] För att söka bland EFF:s prövningar av amerikanska myndigheters befogenheter på internet, se https://www.eff.org/cases.

[12] Information om ACLU:s rättstvister för att pröva amerikanska myndigheters befogenheter återfinns på https://www.aclu.org/defending-our-rights.

[13] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333); BVerfG, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 - Rn. (1-29).

[14] Lennart Johansson, ”Banker och internet” Iustus förlag (Stockholm), 2006.

[15] Jean-Francois Blanchette, ”Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents” MIT Press, 2012.

en leverantör och en konsument, kan både leverantören och konsumenten vara beroende av ett flertal tredjeparter för att transaktionen ska genomföras.

Vidare behandling av ämnesområdet finns i mer eller mindre snävt utförande från bland annat Jennie Grön,[16] Nicolas Bohm,[17] Ross J. Anderson med flera,[18] Axel M. Arnbak.[19] eller Stephanie K Pell och Christofer Soghoian.[20] Lägg märke till att forskningsområdet för säkerhetsekonomi är stort och växer. Vi kan bara använda ett mindre antal källor i detta arbete, som vi komplementerar med erfarenheter från våra egna organisationer.

Ingen juridisk säkerhet vid användning av elektroniska signaturer

Det följande kommer att handla om elektroniska signaturer och elektronisk identifikation. Vi kommer att gå igenom hur konsumenter tvingas bära risken och ansvaret för att tekniska säkerhetsfel uppstår i elektroniska system.

I EU:s förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner[21] läggs bevisbördan för en elektronisk signaturs äkthet (pålitlighet) helt på den som använder den tekniska möjligheten att framställa en elektronisk signatur (gäldenären). Detta förhållande bekräftas i svensk doktrin av Henrik Bengtsson på advokatfirman Delphi.[22]

I EU:s förordning omvänds ifall borgenären använt en ”kvalificerad elektronisk signatur”. Detta begrepp har ingen relevant innebörd i svensk juridik utan finns med i den europeiska lagstiftningen på grund av franska och tyska notarius publicus-funktioner (se Blanchette ovan). Alla elektroniska signaturer i Sverige är så kallade ”okvalificerade” signaturer och flyttar därför risken från tjänsteleverantörer och myndigheter till konsumenter och enskilda.[23]

Den ökade användningen av elektroniska signaturer (till exempel chip-and-pin-kort, Verified by VISA/Mastercode eller internetbankbetalningar), flyttar alltså juridiskt risken för konsumentaktiviteten från betaltjänstleverantören (banken) till konsumenten.[24] Detta har redan drabbat svenska konsumenter negativt i sådan utsträckning att det skrivits om det i media under flera år.[25]

Att den juridiska risken ligger på konsumenten ökar behovet av säkerhet i konsumentens egna verktyg (webbläsare, e-postklient, operativsystem, osv.), så att lösenord, inloggningsuppgifter, kredituppgifter och dylikt inte kan avhändas

Förordning nr 910/2014, artikel 24-26.

Figur 1: Alla tillfällen då enskilda använder e-legitimation flyttas risken och bevisbördan för att transaktionen kommit till stånd på rätt sätt från tjänsteleverantören och myndigheten till den enskilda. I praktiken bör det vara omöjligt för enskilda att bevisa att en teknisk åtgärd hos en myndighet eller tjänsteleverantör gått fel, varför konsumenter är väldigt utsatta i elektroniska miljöer. När banker i sin marknadsföring pratar om ”säker identifiering” menar de att identifieringen är (tekniskt och juridiskt) säker för banker, inte att identifieringen är juridiskt (eller nödvändigtvis tekniskt) säker för konsumenter.

[16] Jennie Grön. ”Framtidens bok – från avtalat ägande till övervakat lån” Examensarbete i civilrätt. Juridiska fakulteten, Uppsala universitet, 2015.

[17] Nicholas Bohm et al, ”Electronic Commerce: Who Carries the Risk of Fraud?” 2000 (3) The Journal of Information, Law and Technology (JILT).

[18] Ross Anderson. ”Why Cryptosystems Fail” ACM. 1st Conf. - Computer and Communication Security 1993; Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, ”Chip and PIN is Broken” 2010 IEEE Symposium on Security and Privacy.

[19] Se ovan fotnot 3.

[20] Stephanie K Pell, Christopher Soghoian. ”Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy” Harvard Journal of Law and Technology, Volume 28, Number 1 Fall 2014.

[21] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

[22] Henrik Bengtsson, advokat, Advokatfirman Delphi, datum okänt, ”Bevisbörda och beviskrav vid invändning om underskriftsförfalskning – särskilt om elektroniska signaturer”.

[23] Post- och telestyrelsens informationssida om kvalificerade elektroniska signaturer: https://www.pts.se/sv/Bransch/Internet/Elektroniska-signaturer/Fragor-och-svar/Kvalificerade-elektroniska-signaturer/

[24] Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, ”Chip and PIN is Broken” 2010 IEEE Symposium on Security and Privacy; se ovan fotnot 22.

[25] Lotta Lille (12 oktober 2012) ”Bedragare stal semesterkassan”, Upsala nya tidning; P1 Plånboken (30 mars 2016).

konsumenten via någon sorts dataintrång. Sådana dataintrång kan till exempel utgöras av att man bereder sig möjlighet att administrera användarens system på avstånd, att man kan utge sig för att vara användarens tjänsteleverantör fastän man inte är det eller att man kan avlyssna trafiken mellan användaren och dess tjänsteleverantör eller internetleverantör.

Exempel på när sådana dataintrång begås finns både från arbete i brottsbekämpande syfte och från kriminella operationer. Här följer några direkt relaterade exempel från båda världarna:

FBI använder remote administration tools (RATs)[a]	Män som spionerar på sina partners med RATs[a]
Tyska och schweiziska polismyndigheter använder Skype-trojaner.[b]	Kriminella använder Skype-trojaner för att stjäla företagshemligheter.[b]
Amerikansk polis låtsas vara tidningar.[c]	Tjuvar låtsas vara banker.[c]

[a] Craig Timberg och Ellen Nakashima (6 december 2013) ”FBI’s search for ‘Mo,’ suspect in bomb threats, highlights use of malware for surveillance”, Washington Post.
[b] Kim Zetter (31 augusti 2009) ”Code for Skype Spyware Released to Thwart Surveillance”, Wired; Graham Cluley (10 oktober 2011) ”German ‘Government’ R2D2 Trojan FAQ”, Naked Security (Sophos).
[c] Mike Carter (27 oktober 2014) ”FBI created fake Seattle Times Web page to nab bomb-threat suspect”, Seattle Times.

[a] Nate Anderson (11 mars 2013)”The Remote Administration Tool is the revolver of the Internet’s Wild West”, Ars Technica.
[b] Doug Olenick (8 februari 2016) ”Skype targeted by T9000 backdoor trojan”, SCMagazine.
[c] Kristoffer Örstadius (28 oktober 2014) ”Vanliga modem lätta att kapa”, Dagens nyheter

Lurendrejeri i elektroniska miljöer är tekniskt fascinerande, och applikationerna av att utnyttja säkerhetsfel i informationssystem är lika många som det finns informationsystem. Vårt urval av exempel är begränsat, och är menat att illustrera att andra länders brottsbekämpande myndigheters redan befintliga arbetsmetoder har direkta motsvarigheter i kriminell verksamhet. Till skillnad från andra verktyg som används av både kriminella och brottsbekämpande myndigheter, till exempel skjutvapen, går det inte att undvika risken att bli utsatt för kriminella verktyg på internet. Hela den tekniska infrastrukturen för internet är byggd med det enda syftet att sätta människor och datorer i kontakt med varandra. Ett skjutvapen som finns på en fysisk plats går att undvika genom att inte besöka den fysiska platsen eller ta sig bort från den fysiska platsen. Detta är inte möjligt i nätverkade miljöer. Den här skillnaden mellan digitala och fysiska vapen är viktig för utredaren att bära med sig.

Det är mycket ogynnsamt för enskilda att berövas både tekniskt och juridiskt skydd vid säkerhetsproblem vid konsumenttransaktioner, och det är en ofta förbisedd omständighet att det juridiska skyddet för konsumenter och enskilda är obefintligt.

Om polisen, eller någon annan myndighet, har ett eget ekonomiskt eller operativt intresse av att hemlighålla, under vilken som helst tidsperiod, mjukvaru- och hårdvarufel som utsätter konsumenter för risk trots att de begagnar sig av tekniskt komplicerade mekanismer för säkerhet, innebär detta att konsumenters och enskildas ytterligare försvagas från en redan svag position. Vi återkommer till detta på sidan 13.

Dessa omständigheter talar emot att låta polisen och andra myndigheter att begagna sig av sanktionerade dataintrång, eftersom dessa metoder per definition (se ovan sidan 2 om definitioner av begrepp) innebär att man riskerar försena möjligheten att upptäcka och åtgärda sårbarheter i IT-system.

Myndigheter bör ges en sådan skyldighet som Post- och telestyrelsen föreslog i sin rapport om ett Säkrare internet i Sverige 2006,[26] nämligen den att kunna kräva in rapporter om sårbarheter för att se till att de snabbast möjligt blir åtgärdade. Det minsta konsumenter och enskilda bör kunna förvänta sig är att inte bära risken för transaktioner som genomförts då konsumenten blivit utsatt för ett säkerhetsfel som orsakas av en part utanför transaktionen, till exempel en IT-brottsling eller en myndighet.

Oklar juridisk säkerhet för tjänster utan elektroniska signaturer

Betaltjänster kräver ofta flera lager av tekniska säkerhetsmekanismer för den enskilde, men det finns också tjänster som det av olika skäl vore otympligt om de krävde sådana säkerhetsmekanismer. Teknisk säkerhet innebär ofta större tröghet vid användningen av ett system, till exempel att konsumenter behöver genomgå fler steg för att logga in, eller behöver begagna sig av extern utrustning (som en dosa eller ett kort) för att komma åt en tjänst.

De flesta tjänster har därför inte samma starka tekniska säkerhet som betaltjänster och e-legitimationstjänster och konsumenten drabbas därför inte av den av lagen omvända bevisbördan. Konsumenten drabbas istället av avtalsrättslig osäkerhet. I svensk rättspraxis är det inte tydligt att konsumenten inte bär risken för en transaktion, även då en elektronisk signatur inte använts.[27]

Jennie Grön har vid Uppsala universitet skrivit ett examensarbete i juridik om enskildas möjligheter att hävda individuella rättigheter och konsumenträttigheter vid boklån i elektroniska miljöer.[28] Hennes slutsatser är att de möjligheter för konsumenter att hävda sina rättigheter som rimligen finns sällan har prövats och att svårigheten i att hävda rättigheterna gör att konsumenter drar sig för att få rättigheterna prövade. Hon menar också att de långa slutkonsumentavtal som är vanliga i amerikansk rätt riskerar att ha normaliserats i Sverige. Därmed har konsumenternas möjligheter att förstå vilka rättigheter de har också minskat.

Det är ofta lättare att komma åt känsliga uppgifter från enskilda genom att attackera sårbarheter i användarnas egen mjukvara, till exempel webbläsaren, appen eller operativsystemet, än genom att attackera tjänsteleverantören. Användaravtalen avskriver dock i regel leverantören från ansvaret för säkerhetsbrister och sårbarheter i mjukvaran, eller gör en prövning av ansvaret avhängig en rättsprocess i någon utländsk jurisdiktion.

Typiska avtalsskrivningar är ”Vi gör vårt bästa för att hålla [tjänsten] säker[,] men vi kan inte garantera det,” åtföljt av en lista med användarens förpliktelser,[29] samt ”alla anspråk, fordringar eller tvister som uppstår gentemot [tjänsten] på grund av eller i anknytning till den här Redogörelsen eller [tjänsten ska lösas] i den federala domstolen för det norra distriktet i Kalifornien eller en

[26] Post- och telestyrelsen. Strategi för ett säkrare Internet i Sverige. PTS-ER-2006:12.
[27] Se ovan fotnot 22.
[28] Se ovan fotnot 16.
[29] Se Facebooks slutanvändaravtal, klausul 3. https://www.facebook.com/legal/terms/update

delstatsdomstol i San Mateo County."[30]

Gröns genomgång är så vitt vi vet ensam i sitt slag, men det finns få anledningar att tro att svenska konsumenters ställning är bättre eller tydligare än den situation som beskrivits för amerikanska konsumenter i Lorrie F Cranors undersökningar av användaravtal i elektroniska miljöer. Cranor kommer tillsammans med Aleecia MacDonald fram till att en genomsnittlig internetanvändare skulle behöva använda 73 timmar per år för att få ens en översiktlig bild av vilka avtalsvillkor den godkänner.[31] I en ytterligare studie av användaravtal i nätreklamsektorn visar att självreglerande mekanismer i sektorn inte fungerar.[32]

EU-kommissionen har i omgångar utrett tjänsteleverantörers och IT-produktleverantörers ansvarsställning i förhållande till konsumenter.[33] I sitt förslag om nya regler för digitalt innehåll på den inre marknaden[34] har man dock avsett att stärka konsumenters rätt att klaga på dåliga bild- eller ljudkvalitet i datorspel och filmer, snarare än att åtgärda riskfördelningen vid säkerhetsfel.

Samrådsanalysen från 2007[35] indikerar, inte helt utan fog, att det vore mycket svårt att införa produktansvar för IT-tjänster som inte till exempel bygger på transparensförpliktelser kring säkerhetsfel och åtgärdanden av desamma i den takt de upptäcks. På sidan 11 utvecklar vi denna tankegång och hur den hamnar i konflikt med de områden utredningen har att ta ställning till.

I praktiken har konsumenter få möjligheter att upptäcka brister av teknisk säkerhetsrelaterad art, och även om de drabbas av säkerhetsrelaterade problem är det inte säkert att de kopplar problemen till en sårbarhet i antingen deras egna eller deras tjänsteleverantörers IT-system. Ett exempel är de över 200 bedrägerier som drabbat Örebrobor i samband med beställningar från OnlinePizza.se våren 2016.[36] Problemet som drabbade de bedragna hade uppenbarligen en teknisk lösning (OnlinePizza.se ändrade sina rutiner för betalning efter att händelsen fått mediauppmärksamhet) men de drabbade agerade i första hand genom att polisanmäla. Sårbarheten i det tekniska systemet för att ta reda på vem som beställt pizza ledde till att personer som egentligen inte ens efterfrågat en relation med det tekniska systemet drabbades negativt. Detta är symptomatiskt för säkerhetsfel i IT-system och förvärras av att säkerhetsfel bara åtgärdas efter storskaliga mediauppbåd. Hade de bedrägeridrabbade varit färre, till exempel tio personer istället för 200, är det osannolikt att det här felet hade åtgärdats.

I de fall Datainspektionen kommer finna det lämpligt att låta personuppgiftsansvariga informera privatpersoner om personuppgiftsincidenter i enligt med artikel 34 i EU:s nya allmänna dataskyddsförordning kan det uppstå en möjlighet för konsumenter att utkräva ansvar, men denna information kommer bara att röra redan inträffade incidenter. Med det avses att skadan kommer redan

Förordning (EU) 2016/679, art 34.

[30] Se Facebooks slutanvändaravtal, klausul 15. Ovan fotnot 29.

[31] Aleecia M. McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue.

[32] Lorrie F Cranor,. et al. (2014). Are they worth reading? an in-depth analysis of online advertising companies' privacy policies. Rochester, NY: Social Science Research Network.

[33] EU-kommissionen (2006). COM (2006) 744 final. Green Paper on the Review of the Consumer Acquis; EU-kommissionen (2015). Public consultation on contract rules for online purchases of digital content and tangible goods.

[34] EU-kommissionen (2015) COM(2015)634 Förslag till Europaparlamentets och rådets direktivet om vissa aspekter på avtal om tillhandahållande av digitalt innehåll.

[35] EU-kommissionen (2007) Detailed analysis of responses to the European Commission Green Paper on Consumer Rights Reform.

[36] Mattias Frödén (23 april 2016) "Härvan växer - hundratals offer för pizzabluffen", Nerikes allehanda.

vara skedd när konsumenten eventuellt kan ges en möjlighet att agera i sitt eget intresse.

Även om EU-kommissionens förslag i teorin kan ge vissa ytterligare garantier om säkerhet, återstår problemet att konsumenter, även om de mot all förmodan informeras om ett säkerhetsproblem eller sårbarhet i sin IT-produkt, i praktiken saknar incitament eller möjligheter att hävda sina rättigheter. I EU-området är det i stort sett bara den tyska konsumentföreningen Verbraucherzentrale Bundesverband som drivit konsumentfrågor för digitala miljöer i domstol, och då kring frågor som appbutiker[37] och möjligheter att sälja vidare datorspel.[38] När Sveriges konsumenter försökt få digitala avtal prövade av Konsumentverket, har bemötandet från myndigheten varit att frågan inte ligger på deras bord.[39]

Förflyttningen av IT-säkerhetskompetenser från Post- och telestyrelsen till Myndigheten för samhällsskydd och beredskap 2009 har inneburit ett ytterligare försvagande av konsumentens ställning, eftersom det näringspolitiska perspektivet gradvis fallit bort ur behandlingen av vad IT-säkerhet är och ska vara. År 2006 föreslog Post- och telestyrelsen obligatorisk sårbarhetsrapportering för att möjliggöra snabba patchar.[40] Idag utreds hur de brottsbekämpande myndigheterna ska beredas tillgång till metoder att utnyttja sårbarheter.

Dir. 2016:20, Dir. 2016:36, Prop 2014/15:109 (kapitel 8).

Konsumenternas representation från myndigheterna minskar alltså, samtidigt som konsumenter blir allt mer utsatta. Det gäller inte bara i e-handel och e-transaktioner utan även för andra tjänster som konsumenter måste använda (till exempel elektricitet, vatten, och gas), eller som enskilda i egenskap av medborgare måste associera sig med (skolor, universitet, Skatteverket, och dylikt), och som i ökad utsträckning har elektroniska eller internetuppkopplade element. Närmare behandling av dessa problem ligger utanför den här textens ramar, men observationerna om hur man förbättrar säkerhet på sidorna 11– gäller även i dessa sektorer.

Det här är så klart är en politisk prioritering – frågan är bara hur medveten den varit.

Vi menar att utredaren behöver lyfta detta perspektiv så att det inte är av okunskap och oförståelse som konsumenternas ställning försämras. Vi är medvetna om att utredarens uppdrag knappast kan utgöra mer än en liten pusselbit i det större sammanhang där konsumenter och enskilda gradvis har hamnat i väldigt svag ställning i förhållande till företag, stater och myndigheter, men utredarens uppdrag kan ändå vara en viktig pusselbit, inte minst för att utredaren har möjlighet att genomlysa problemen.

Utredningens uppdrag att ta fram metoder för de brottsbekämpande myndigheterna att genomföra sanktionerade dataintrång spär på den redan svaga rättsliga och tekniska ställning enskilda och konsumenter har i digitala miljöer.

Inga konsumentgarantier för integritet och tillförlitlighet

Dataskydd.net har frågat Datainspektionen, Reklamombudsmannen, Myndigheten för samhällsskydd och beredskap samt Post- och telestyrelsen om det

[37] Verbraucherzentrale Bundesverband. (6 juni 2013). ”Samsung App-Store: Viele Klauseln unzulässig.”

[38] Spielerecht.de, Osborne Clarke Publication number 1506540 ”Update: Valve May Prohibit Steam Account Transfers – German Judgment”, mars 2014.

[39] Jan Bertoft (29 april 2015) ”Se upp för Blocket”, Egen blogg för ordföranden i Sveriges konsumenter.

[40] Se ovan fotnot 26.

i svensk rätt finns bestämmelser som skyddar konsumenter från den omständighet att ett kommersiellt företag kringgår tekniska säkerhetsmekanismer som konsumenten installerat i sin tekniska utrustning, till exempel en adblocker som installerats i webbläsaren. Alla myndigheter har bekräftat att någon sådan rätt inte finns. Även Reklamombudsmannen och Konsumentvägledningen i Enköpings kommun hävdar att det inte finns något sådant skydd.[41]

Även en säkerhetsmedveten privatpersoner som i största möjliga mån försöker anpassa sitt datoranvändande efter den rådande hotbilden, och som inför extra skyddsmekanismer i sin elektroniska utrustningen för att till exempel inte bli utsatt för phishing-attacker, virus, DNS-spoofing eller kriminella trojaner, behöver alltså samtidigt parera både stater och företag utan att ha en enda lagbestämmelse på sin sida.

Kringgående av enskildas egna säkerhetsåtgärder – till exempel den numera populära uppmaningen till enskilda teknikanvändare att verifiera att webbplatser som den enskilda besöker begagnar sig av TLS eller SSL – är till och med en normal och accepterad säkerhetsåtgärd i många företagsnät, då till företagets snarare än till den enskildes fördel.[42]

Den nederländske jur dr Axel Arnbaks avhandling om säkerhet och ekonomi i europeisk lagstiftning går igenom hur lagstiftaren ofta fokuserat på IT-systemens tillgänglighet (till exempel åtgärder som garanterar en viss upp-tid på en server, så som att en hemsida eller databas är tillgänglig och går att nå över ett kommunikationsnät) men eftersatt integritet och tillförlitlighet, när lagstiftaren utarbetat lagstiftning om säkerhet i elektroniska miljöer. Arnbak menar att detta lett till att den sortens säkerhet som är viktigast för konsumenter inte har fått något stort utrymme i säkerhetslagstiftningen.[43]

I svenska förarbeten finns en företrädelsevis stark fokus på tillgänglighet, och om tillförlitlighet tas upp alls, är den definierad utifrån staters och företags perspektiv snarare än enskilda individers.[44] Den närmaste motsvarande svenska doktrinen är jur dr Markus Naarttajärvis avhandling om proportionalitetskrav och preventiva tvångsmedel, där han tagit upp att enskildas intressen i allt högre utsträckning avfärdas som en individuell angelägenhet, varför dessa intressen får stå tillbaka för det allmännas, till exempel brottsbekämpande myndigheters, intressen.[45]

Utredningsuppdraget att framta förslag för hur de brottsbekämpande myndigheterna ska få möjlighet att utföra sanktionerade dataintrång och genomföra allt mer ingripande åtgärder i enskildas elektroniska miljöer är ytterligare ett led i eftersättandet av integritet och tillförlitlighet som lika viktiga delar av säkerhetsbegreppet som tillgängligheten.

Ett realiserande av de förslag som utredningens uppdragits ta fram kommer att ytterligare försvaga konsumenters och enskildas redan svaga ställning i förhållande till både tjänsteleverantörer och myndigheter, när konsumenter och enskilda i själva verket borde tilldelas ett bättre och starkare skydd.

”Transport Layer Security (TLS), ’transportlagersäkerhet’, är ett kryptografiskt kommunikationsprotokoll som är en öppen standard för säkert utbyte av krypterad information mellan datorsystem. TLS är en vidareutveckling av version 3 av SSL-protokollet[.]”, via Wikipedia. TLS eller SSL-kryptering gör så att en internetleverantör eller annan mellanhand inte kan se exakt vad kommunikationen innehåller. I de flesta moderna webbläsare markeras att en hemsida använder TLS eller SSL-kryptering genom ett litet grönt lås längst uppe till vänster i raden för webbplatsadressen (URL:en).

41 Dataskydd.net, (15 maj 2016) ”Lågt skydd för konsumenter som vill stärka sin säkerhet”
42 Stuart Burns (20 maj 2016) ”Hacked in a public space? Thanks, HTTPS”, The Register.
43 Se ovan fotnot 3.
44 SOU 2013:39, Europarådets konvention om it-relaterad brottslighet; jfr också Myndigheten för samhällsskydd och beredskaps arbete mot DDOS-attacker, eller inrikesministerns insatser mot DDOS-attacker.
45 Markus Naarttijärvi. Doktorsavhandling, Umeå universitet, 2013. ”För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel”

Husrannsakan på distans och i en dator

I det följande hanterar vi både husrannsakan på distans och husrannsakan i en dator. Anledningen till detta är att konsekvenserna för konsumentsäkerhet och säkerhet för enskilda vid elektroniska kontakter med myndigheter eller andra enskilda i teknisk och juridisk mening omgärdas av samma typer av problem. Oavsett vad man kallar arbetsmetoden att olovligen (i förhållande till hur IT-systemet varit tänkt att användas av dess ägare) utnyttja funktioner i ett IT-system försvagar metoden konsumenters och enskildas ställning.

Säkerhetsförbättringar och ekonomi

Vid utveckling och underhåll av mjukvara och hårdvara finns ett antal större utmaningar som är väl kartlagda. Faktum är att det främst var utmaningar vid utveckling och underhåll av IT-system som motiverade den första svenska dataintrångsbestämmelsen år 1972[46] och Europarådets rekommendation om IT-brottslighet från 1989.[47] I den för rekommendationen bakomliggande utredningen skriver man att det juridiska skyddet för systeminnehavaren är det som kan skydda vad som av ekonomiska skäl inte är rimligt att skydda på teknisk väg.

Näringslivet har utvecklat andra metoder för säkerhet än att förlita sig på lagstiftningen. Istället för att ty sig till straffrätten, läggs idag en betydligt större tonvikt på öppenhet med och små gradvisa förbättringar av hantering av IT-säkerhetens utmaningar.

Bug bounty awards, ett sätt att dela ut belöningar till dem som hittar sårbarheter i IT-system, har till exempel blivit vanliga.[48] Utbyte av information om sårbarheter inom företagsnätverk som ISAC:s har blivit ett vanligare sätt att snabbt ta hand om säkerhetsproblem som annars skulle drabba många i samma industri.[49]

Det finns även standardiserade databaser där kända sårbarheter publiceras för hela världen att granska och se, till exempel MITRE-institutets Common Vulnerabilities and Exposures-system (CVE). Öppen publicering (under vissa villkor) ses ofta som en förutsättning för att säkerhetsproblemen som följer av sårbarheterna ska åtgärdas.

Till skillnad från många äldre akademiska discipliner präglas dataveten-skapen och säkerhetsekonomisk forskning av öppna publiceringar: det är till exempel vanligare att forskare presenterar sina resultat på konferenser än att de låter publicera sig i slutna tidskrifter. WEIS, IEEE Security and Privacy, Chaos Communication Congress eller Blackhat är exempel på sådana konferenser.

Att det är viktigt med individuella rättigheter och säkerhet för att ekonomin ska fungera bättre är också tydligt från många undersökningar av hur privatpersoner förhåller sig till elektroniska miljöer. Amerikanska näringsdepartementet konstaterade så sent som våren 2016 att allt fler privatpersoner drar sig för att använda

Common Vulnerabilities and Exposures-system (CVE):

CVE-systemet illustrerar de geopolitiska implikationerna av hur IT-säkerhet i normalfallet hanteras av näringslivet idag. Det faktum att världens största databas för kända sårbarheter är belägen på amerikanska servrar väcker frågeställningen om den amerikanska regeringen tillsammans med MITRE-institutet ser till att vissa sårbarheter, som de själv vill utnyttja, inte listas i databasen. Om så är fallet kan de amerikanska myndigheterna ge sig själva ett försprång vid ”offensiv IT-säkerhet”, det vill säga sådana militära operationer som innebär att man hotar andra länders IT-säkerhet. En möjlig lösning på dilemmat är så klart att man ser till att det finns öppna databaser i flera olika länder, gärna sådana länder som inte omedelbart misstänks vara allierade med USA. Det skulle stärka förtroendet för näringslivets och staternas förmåga och vilja att åtgärda säkerhetsproblem istället för att bevara dem.

[46] SOU 1972:47, Data och integritet.

[47] Council of Europe, Recommendation (89) 9 on computer-related crime and and final report of the European Committee of Crime Problems (1989).

[48] Se till exempel https://bugcrowd.com/list-of-bug-bounty-programs

[49] CIRCL.lu, Malware Information Sharing Platform MISP - A Threat Sharing Platform. https://www.circl.lu/services/misp-malware-information-sharing-platform/; National Council of Information Sharing and Analysis Centers, http://www.nationalisacs.org/

elektroniska tjänster på grund av otillräckliga garantier för säkerhet och skydd för privata uppgifter.[50] Till exempel Internetstiftelsens andra årliga utredning om svenskarnas förhållande till privatliv i elektroniska miljöer ger skäl att inte avfärda möjligheten att oron för säkerhet och dataläckor kan vara tilltagande även i Sverige.[51] Också internationella enkätundersökningar visar att oron för säkerhet och dataskydd bland privatpersoner ökar, bland annat med effekten att enskilda inte gör saker de annars skulle göra eller att de slutar göra saker som de tidigare har gjort.[52]

Projektet DigiTrust vid Lunds universitet avslutades 2014 med en skrift där man beskriver förutsättningarna för tillit i digitala miljöer. Forskarna drar slutsatsen att inte bara teknisk säkerhet är viktig för enskildas tillit, utan också vilka juridiska skydd och vilket allmänt intryck som enskilda har av de digitala miljöerna.[53]

Då den tekniska säkerheten av både datavetenskapliga och ekonomiska skäl är svår att garantera fullt ut, och den juridiska säkerheten som ovan angivits i många fall är obefintlig, måste det antas vara riskfyllt att ge de brottsbekämpande myndigheter tillgång till sådana befogenheter som av sin natur förutsätter att tekniska säkerhetsbrister inte åtgärdas.

Sårbarheter och ekonomi

Sanktionerade dataintrång (se ovan sidan 2) kräver antingen att lagar och tekniska standarder medger att produkter utrustas med en metod för polisen att ta sig in i produkterna på distans eller att polisen eller någon annan utvecklar en möjlighet att utnyttja sårbarheter i den rannsakades elektroniska utrustning för att avläsa data på distans. Dessa saker behöver behandlas var för sig:

Inbyggda tekniska metoder för husrannsakan på distans och i en dator

Att utrusta produkter med en metod för polisen att ta sig in i IT-produkter på distans är oftast omnämnt som att ”efterfråga en bakdörr”. Idéen har avfärdats i USA,[54] Frankrike[55] och Nederländerna.[56] I Tyskland har konstitutionsdomstolen i två fall begränsat möjligheterna för myndigheter att efterfråga eller orsaka sämre teknisk säkerhet genom sanktionerade dataintrång, med hänvisning till personlighetsrättigheter.[57] Även Europol är emot tanken på att produkter ska utrustas med inbyggda metoder för polisen att avlyssna.[58]

Med hänvisning till fotnötterna 54–58 behandlar vi inte frågan vidare.

---

[50] United States Department of Commerce, National Telecommunications and Information Administration, ”Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities”, 13 maj 2016.

[51] Internetstiftelsen i samarbete med Insight Intelligence och SICS samt svenska näringslivsaktörer och Stockholms landsting, Delade meningar 2, mars 2016.

[52] 2016 CIGI-Ipsos Global Survey on Internet Security and Trust.

[53] Stefan Larsson och Per Runesson (ed), ”Digitrust: Tillit i det digitala” Lunds universitet juni 2014.

[54] Vita huset, Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, 12 december 2013.

[55] Guillaume Champeau (13 januari 2016) ”Chiffrement : le gouvernement rejette les backdoors”, Numerama.

[56] Matthijs R. Koot (5 januari 2016). ”Full translation of the Dutch government’s statement on encryption” Cyberwar.

[57] Se ovan fotnot 13.

[58] Europol, Director’s Speech at the conference: Privacy in the Digital Age of Encryption and Anonymity Online, Haag, Nederländerna, 19 maj 2016.

Utnyttjande av sårbarheter för husrannsakan på distans och i en dator

I fråga om det andra tillvägagångssättet har den politiska utvecklingen på hög nivå inte kommit lika långt.

Riktad övervakning är i princip mer fördelaktigt för individen ur ett mänskligt perspektiv än massövervakning.[59]

Även vid riktad övervakning krävs att tvångsåtgärden är strikt nödvändig, med vilket Europadomstolen senaste 12 januari 2016 understrukit att de inte menar enbart ”operationellt lämplig”.[60] Den tyska konstitutionsdomstolens bedömningar av metoder för utnyttjande av sårbarheter för att på distans ta sig in i enskildas IT-system ställer upp strikta krav på myndigheter som vill begagna sig av sådana metoder med avseende på tillfällen då sådana metoder kan tänkas vara tillåtna (mycket allvarliga brott, och vid konkret misstanke riktad mot en väl definierad aktör) och rättssäkerhet (proportionalitet, dokumentation, insyn, föregående prövning, information till den utsatte, och så vidare).

I Sverige saknas till vår vetskap specifika behandlingar av rättssäkerhetsfrågor vid polisiära insatser efter 2006.[61]

Figur 2: Ursprungscitatet från Stockholmspolisens IT-brottsansvarige i P3 Dokumentär ”Svenska hackers” (2008) lyder ”*Vill du ha problem, ge grabben ett modem*”. Bild från http://xkcd.com/1597/ CC-BY-NC 2.5

Det finns vidare och relevanta observationer att göra om metoder för sanktionerade dataintrång:

En vanlig fysisk husrannsakan går över när de brottsbekämpande myndigheterna lämnar den fysiska platsen, men en elektronisk husrannsakan går inte över förrän de tekniska åtgärder som vidtagits av de brottsbekämpande myndigheterna görs ogjorda på de datorer som de tekniska åtgärderna utförts på. Utredaren kan jämföra med datorvirus, som inte försvinner från den drabbades dator förrän ett antivirusprogram letat fram och tagit bort den skadliga koden, eller man har ominstallerat sitt operativsystem.

Utan rutiner för underrättelser till den som är föremål för åtgärden samt krav på att det avslöjas hur den tekniska åtgärden genomförts, blir ingreppet i den enskildes sfär mycket allvarligare än en motsvarande fysisk husrannsakan, då åtgärden inte kan upphöra utan att den utsatte bereds möjlighet att avbryta åtgärden.

Den kan vara svårt (om inte omöjligt), rent tekniskt, att säkerställa sig om att den metod man använt för att nå ett IT-system på distans bara faktiskt når det IT-system som det är avsett för. Otillbörlig spridning av metoder för att utnyttja sårbarheter skedde till exempel i Tyskland 2011,[62] och för de oavsiktligen drabbade finns ingen hjälp att få så länge det inte är känt hur man kan laga det introducerade säkerhetsproblemet. Dessa för åtgärden utomstående parter hamnar, utan väldigt effektiva transparensmekanismer kring myndigheternas verksamhet, i sådan ställning som vi på sidan 13 angivit att de flesta länder som övervägt frågan finner oönskvärt.

Vi återvänder i texten om ”revolving doors” och marknadsföring på sidan 15 till varför det kan vara svårare än man vill tro att säkerställa en tillräcklig och

[59] Council of Europe, Parliamentary Assembly, Resolution 2045 (2015) ”Mass surveillance” Text adopted by the Assembly on 21 April 2015 (12th Sitting), med tillhörande Recommendation 2067 (2015).

[60] Para. 75, Europadomstolen, Szabo och Vissy v Hungary (Application no. 37138/14).

[61] SOU 2006:98, Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.

[62] Graham Cluley (10 oktober 2011) ”German ‘Government’ R2D2 Trojan FAQ”, Naked Security (Sophos).

adekvat nivå av transparens för att inte orsaka fler säkerhetsproblem än man åtgärdar.

Om man ändå väljer att gå vidare med förslag om husrannsakan på distans, har vi följande fyra krav (se också sidan 23):

1. Så länge konsumenter bär risken för, eller har bevisbördan då, ekonomiska transaktioner eller andra interaktioner i elektroniska miljöer går fel, så bör de brottsbekämpande myndigheterna över huvud taget inte ägna sig åt verksamhet som försämrar den tekniska säkerheten i sådana verktyg som konsumenter i ökande utsträckning måste använda för att delta i marknaden, socialt liv och myndighetskontakter. Artikel 169(4) TFEU ger den svenska lagstiftaren utrymmet att ta bort presumptionen att bevisbördan och risken för användning av elektroniska signaturer ligger på konsumenten.

2. Ingen åtgärd ska vidtas utan föregående prövning i en oberoende instans. Den oberoende instansen ska få tillräckligt med information för att göra en självständig bedömning av nödvändigheten och proportionaliteten i åtgärden.[63] Informationen ska innefatta en redovisning av hur myndigheterna tekniskt kommer att genomföra och avsluta husrannsakan. Den ska också innefatta vad myndigheterna letar efter och hur de ska undvika att lägga beslag på sådant de inte letar efter. Dessa regler ska gälla både för husrannsakan i en dator de befinner sig i fysisk närhet av och husrannsakan på distans.

3. Efter det att de brottsbekämpande myndigheterna använt tvångsmedlet, bör metoden för hur de brottsbekämpande myndigheterna använt sig av en sårbarhet, samt sårbarheten som sådan, redovisas.[64] Detta krav bör ställas för att underlätta åtgärdande av sårbarheten för den stora majoriteten laglydiga användare av elektroniska verktyg. Kravet gör också att myndigheterna inte använder sig av verktyget i onödan. Om detta krav inte finns med i lagstiftningen innebär det att den som utsatts för tvångsmedlet inte kan avbryta tvångsmedlet: om de brottsbekämpande myndigheterna installerat en metod för dataintrång utan att avslöja hur de har gjort detta kan den som utsatts för intrånget inte avbryta intrånget.

4. De brottsbekämpande myndigheterna bör inte få begagna sig av 0-days, eftersom dessa säkerhetsproblem ännu inte är kända och därför inte kan åtgärdas. Om de brottsbekämpande myndigheterna får kännedom om en sådan sårbarhet eller sådan metod för att utnyttja en sårbarhet bör de åläggas med ett absolut krav att avslöja felet för de parter som kan åtgärda felet för den absoluta majoriteten laglydiga individer.

Vi menar att konstitutionella och människorättsliga prövningar av den här frågan ger ett för begränsat perspektiv. Utanför (vissa delar av utländsk) akademi saknas det huvudsakligen analyser av de ekonomiska och konsumenträttsliga aspekterna av polisiära åtgärder, trots att bestämmelser om myndigheters befogenheter i allra högsta grad påverkar näringslivets prioriteringar. De huvudsakliga problemen med stora befogenheter för brottsbekämpande myndigheter i digitala miljöer är affärsrättsliga eller konsumenträttsliga.

Det är också värt att nämna att den tyska konstitutionsdomstolen gör sina uttalanden mot en bakgrund av att nästan 80% av alla transaktioner i Tyskland

[63] Europadomstolen, Zakharov v. Russia (Application no. 47143/06).

[64] Steven M. Bellovin, Matt Blaze, Sandy Clark, Susan Landau, ”Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet”. Privacy Legal Scholars Conference, June 2013.

genomförs med kontanter,[65] mot 20% i Sverige.[66] Bara ett fåtal procent av tyska befolkningen använder e-legitimation på grund av oro för säkerhet och dataskydd. I Tyskland är det möjligt för en konsument som vill kunna ta till vara på sina rättigheter att göra det genom att inte delta i den digitala ekonomin och förvaltningen. I Sverige finns en uttalad strategi att få människor att använda e-förvaltning och elektroniska betalmedel,[67] som gör det svårt för enskilda att bevara de rättigheter de har i fysiska miljöer som de inte har i elektroniska miljöer.

De ovanstående styckena om konsumenträtt, elektroniska signaturer och avtal för elektroniska tjänster på sidorna 4, 5 och 7 hoppas vi har illustrerat konsumenters utsatta ställning och hur den riskerar att bli ännu mer utsatt om reglerna för husrannsakan utformas på ett sådant sätt som föreslås i utredningsdirektiven. Nu följer istället två behandlingar om näringslivet och hur de brottsbekämpande myndigheterna riskerar att bidra till sådana prioriteringar för näringslivets aktörer som inte är i konsumentens bästa intresse.

”Revolving-doors” och marknadsföring i IT-säkerhetsindustrin

Ett ytterligare övervägande som utredningen behöver göra i förhållande till utnyttjande av sårbarheter i IT-system, är det så kallade ”revolving doors”-problemet. Det finns idag ett relativt stort antal företag som professionellt ägnar sig åt att ta fram metoder för brottsbekämpande myndigheter och underrättelsetjänster att utföra sanktionerade dataintrång. Dessa företag drivs inte sällan av och med personer som kommer från offentlig sektor, till exempel från underrättelsetjänster eller från de brottsbekämpande myndigheterna.[68] Företagen rekryterar tidigare offentliganställda, och utvecklar eller köper in metoder att utnyttja sårbarheter på uppdrag av offentlig sektor.

För myndigheterna finns det fördelar med att outsource:a verksamheten. Privat sektor omfattas inte av några krav på transparens och offentlighet. Det gör att varken företag eller myndigheter behöver redovisa om de har kunskap om metoder för att utnyttja sårbarheter. Marknaden för kunskap om metoder för att utnyttja sårbarheter är delvis kartlagd och delvis vit,[69] men den är ofta också inte vit och inte kartlagd. De företag som hjälper brottsbekämpande myndigheter hitta sårbarheter i elektroniska produkter som används av slutkonsumenter har dock bevisligen haft att göra med sådana sårbarheter som också används vid aktiviteter som skadar enskildas och konsumenters intressen.[70] Behovet av regler för denna marknad har lyfts i europeiska sammanhang av bland andra europeiska dataskyddstillsynsmannen,[71] men i Sverige saknas en sådan diskussion.

[65] Philip Oltermann (8 februari 2016) ”German plan to impose limit on cash transactions met with fierce resistance”, The Guardian.

[66] Sara L Bränström (4 mars 2016) ”Riksbanken: Då blir Sverige kontantlöst”, Svenska dagbladet.

[67] Se till exempel http://www.kontantupproret.se/, E-delegationens utredningar eller Digitaliseringskommissionen.

[68] Andy Greenberg (21 March 2012). ”Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)” Forbes; Adrianne Jeffries (13 September 2013). ”Meet Hacking Team, the company that helps the police hack you” The Verge; Vernon Silver (8 november 2012) ”MJM as Personified Evil Says Spyware Saves Lives Not Kills Them” Bloomberg; Der Spiegel, 9 november 2014 ”BND will Informationen ueber Software-Sicherheitsluecken einkaufen”.

[69] Se ovan fotnot 68.

[70] Peter Pi (7 juli 2015) ”Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak”, Trendlabs Security Intelligence Blogs.

[71] EDPS, Opinion 8/2015: Dissemination and use of intrusive surveillance technologies.

Eftersom de mässor och konferenser som äger rum för försäljning och marknadsföring av dataintrångsprodukter omgärdas av sekretess (antingen via offentliga sekretessregler eller genom *non-disclosure agreements*)[72] har det visat sig vara svårt att få en bild av vad marknaden är, vem som utvecklar saker, till vilket pris och till vilka sårbarheterna säljs.

När det väl finns företag som ägnar sig åt att förmedla metoder för utnyttjande av sårbarheter i IT-system till brottsbekämpande myndigheter, blir dessa företag en egen intressegrupp som utövar politiskt inflytande på de brottsbekämpande myndigheterna och på politiker. Vid Torontos universitet i Kanada, har CitizenLab-gruppen kartlagt vad de menar utgör ett ”*cyber-war industrial complex*” som omsätter åtskilliga tiotals miljarder dollar per år.[73] Företagens egenintresse kan antas vara att framställa sig som ovärderliga och nödvändiga för effektiv brottsbekämpande verksamhet, eftersom deras huvudsakliga intäktskälla är just samarbete med brottsbekämpande myndigheter.

Kontakter med dessa företag går sannolikt inte att undvika, men kontakten kan vara mer eller mindre direkt. Låt oss säga polismyndigheten inte direkt förvärvar sårbarheter eller metoder att använda sårbarheter från privat sektor, utan att metoderna förvärvas från andra myndigheter, som kanske i sin tur har kontakt med utländska myndigheter. De sårbarheter som kan användas för att skada konsumenters och enskildas intressen kan då täckas då av försvarssekretess i flera led, vilket gör att det inte går att spåra varifrån metoderna kommer, vem som har utvecklat dem eller ens vad de mer exakt gör.

För all verksamhet relaterad till sanktionerade dataintrång är kontakterna med privat sektor så pass utbredda att det i princip är otänkbart att svenska skattemedel inte skulle gå till vad som enklast kan beskrivas som en osäkerhetsindustri. Här kan det vara hjälpsamt med några exempel:

---

[72] Ryan Gallagher (1 november 2011) ”Governments turn to hacking techniques for surveillance of citizens” The Guardian.

[73] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “For Their Eyes Only: The Commercialization of Digital Spying,” Citizen Lab Research Brief No. 17, April 2013; Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “You Only Click Twice: FinFisher’s Global Proliferation,” Citizen Lab Research Brief No. 15, March 2013; Morgan Marquis-Boire (lead technical research) and Jakub Dalek (lead technical research), Sarah McKune (lead legal research), Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman, “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,” Citizen Lab Research Brief No. 13, January 2013; Övriga publikationer på CitizenLab Publications: https://citizenlab.org/publications/

I USA har brottsbekämpande myndigheters förvärv av produkter för sanktionerade dataintrång varit omskrivna, mindre på grund av transparens kring inköpen som med anledning av läckor och informella tillkännagivelser.[a]

Vi har redan tidigare exemplifierat tyska och schweiziska polisens inköp av trojaner.[b]

I Nederländerna köpte underrättelsetjänsten 2013 in mjukvaran Argo II, som de vid tillfället inte hade laglig rätt att använda. På grund av Snowden-läckorna ägde de förväntade lagändringarna inte rum, och fortfarande läggs nederländska skattepengar på ett system som är olagligt.[c]

[a] Se t ex Bloomborg (30 mars 2016) ”FBI Worked With Israel’s Cellebrite to Crack iPhone”; Joseph Cox (6 juli 2015) ”The FBI Spent $775K on Hacking Team’s Spy Tools Since 2011”, Wired. Se även nedan fotnot 74.

[b] Se ovan sida 6.

[c] Michael Persson (9 november 2013) ”Nederland bestelt een nog verboden spionagesysteem”, Volkskrant; Nederlandse overheid, Ministerie van Defensie, ”Gegevens verwerken met ARGO II”.

I vissa delar av IT-säkerhetsbranschen är det häftigt att kunna förstöra eller olovligen ta sig in i ett IT-system. Att vinna så kallade ”capture the flags”-tävlingar (en tävling där den som först lyckas utnyttja en sårbarhet vinner) ger status gentemot andra IT-säkerhetsexperter eftersom de ökar förståelsen för vilka sårbarheter och möjligheter att utnyttja sårbarheter som finns i ett system, men också hur man kan åtgärda sårbarheterna.

Vi är oroliga för att de brottsbekämpande myndigheterna har ”smittats” av att det är häftigt att olovligen ta sig in i IT-system och att det går att göra många saker med datorer.[74] Att det idag finns en stor industri som jobbar med att övertyga brottsbekämpande myndigheter om att det är häftigt att ta sig in i IT-system[75] får myndigheterna att låta bli att överväga tråkigare och tekniskt mindre spektakulära utredningsmetoder.

I försvarssammanhang har offensiv IT-säkerhet, det vill säga militärt sanktionerade dataintrång, framställts som en billigare metod att bedriva säkerhetsarbete i nätmiljöer än att ägna sig åt förebyggande verksamhet och transparens.

Vi ifrågasätter detta mot bakgrund av den förståelse för säkerhet och ekonomi som utvecklats inom både forskning och näringsliv under de senaste två decennierna (se ovan på sidan 11 om säkerhetsförbättringar och ekonomi).

Vi menar att det istället rör sig om en psykologisk effekt, där näringslivets metoder för att gradvis och i små steg förbättra säkerheten i IT-system får de statliga myndigheterna att vilja delta i sådant som är coolt, men på sådana villkor att effekten med stegvisa förbättringar och åtgärdande av säkerhetsfel uteblir. Marknaden för polisnära tjänster har sedan växt på ett sådant sätt att man i ännu högre utsträckning inspireras fortsätta arbeta med samma metoder.

I Christopher Soghoians och Stephanie K Pells genomgång av säkerhet i mobiltelefonnätverk,[76] exemplifieras både myndigheters och lagstiftares felaktiga

Snowden-läckorna

”Snowden-läckorna” hänvisar till den större läcka av information om amerikanska underrättelsetjänsten National Security Agencies offensiva IT-säkerhetsverksamhet som skedde i juni 2013. Läckorna avslöjade avancerade attacker mot sociala nätverk och krypteringssystem, avlyssning av stamnät och internetknutpunkter samt samröret mellan den amerikanska underrättelsetjänsten och utländska partners. Läckorna har varit betydelsefulla på det sätt att de givit en förståelse för hur säkerhetsproblem i digitala miljöer utnyttjas av stater. De har blivit mycket omdiskuterade, både i medier och bland lagstiftare i många länder. Ledande tidskrifter i rapporteringen var initialt The Guardian och Washington Post.

74 Bruce Schneier (25 februari 2011) ”HBGary and the Future of the IT Security Industry”, schneier.com.

75 Se ovan fotnot 68.

76 Se ovan fotnot 20.

långsiktiga prioriteringar för IT-säkerhet tydligt. Författarna framhåller, i enlighet med Axel Arnbak,[77] att lagstiftaren borde ha fokuserat på integritet och tillförlitlighet för konsumenter och enskilda i basinfrastrukturen istället för att förbjuda försäljning av viss utrustning som möjliggör utnyttjande av sårbarheter i basinfrastrukturen till allmänheten (dock utan att förbjuda sådan försäljning till brottsbekämpande myndigheter och försvarsrelaterade myndigheter).

Det finns en påtaglig risk att den svenska lagstiftaren och brottsbekämpande myndigheter via privilegierad access till forum som allmänheten inte har tillträde till, blir utsatta för marknadsföring som ger dem en orealistisk bild av vad som fungerar bra för att lösa brott, och vad som ligger i allmänhetens intresse.

Marknadskrafter och lobbyism ska inte underskattas: marknaden för utnyttjande av sårbarheter är lukrativ och växer, och utredaren har ett val om den vill lägga tonvikt på att gynna denna marknad, eller om utredaren istället vill föreslå en väg framåt som innebär ett större fokus på integritet och tillförlitlighet (se ovan sidan 9).

Beslag av information

Vi är tveksamma inför att ge de brottsbekämpande myndigheterna möjlighet att beslagta elektroniskt lagrad information. Uppdragsgivaren ser ut att ha motiverats av två fall då medier publicerat pixellerade bilder.[78] I varje fall skulle den sortens regler som utredningsdirektiven bett att få utvärderade kunna användas för att kringgå Högsta domstolens beslut om förbud mot beslag av Aftonbladets hårddiskar i augusti 2015.

Vid utformningen av rättspolitiska åtgärder behöver utredaren noggrant undersöka i vilken utsträckning utredaren ger incitament för näringslivet att utvecklas, eller inte utvecklas, i olika riktningar. Genom lagstiftningen kan näringslivet indirekt styras att välja vissa, för individer mindre gynnsamma, säkerhetslösningar.[79]

I tidigare svenska utredningar har det framställts som positivt att näringslivet kan utveckla specialiserade lösningar för aktiviteter som inte ligger i enskildas och allmänhetens intresse. I en utredning om datalagring från 2007 antog till exempel utredaren att dedikerade datalagringstjänster kunde hjälpa småföretag hantera kostnaden för datalagring.[80] Den resulterande datalagringsindustrin[81] hjälpte sedan med och bidrog till processer för att utveckla tekniska protokoll för datautlämning som gick längre än vad lagstiftningen krävde, till exempel genom att möjliggöra direktåtkomst för brottsbekämpande myndigheter till internetoperatörers information om enskilda (jämför styckena på sidan 15 om revolving doors och marknadsföring).[82] Allmänheten, det vill säga konsumenter och enskilda i Sverige och annorstädes, hade inte fått kännedom om denna utveckling om inte en näringslivsaktör tydligt agerat mot, i detta fall, Säker-

[77] Se ovan fotnot 3.

[78] Tronarp, Ornerud, Hagberg (18 augusti 2015) ”Högsta domstolen stoppar husrannsakan på Aftonbladet”, Aftonbladet; Geronimo Åkerlund (21 januari 2016) ”Därför pixlar vi”, SVT.

[79] Se ovan fotnot 24 och 20.

[80] SOU 2007:76. Lagring av trafikuppgifter för brottsbekämpning.

[81] Tor Borrhed, ”Maintrac summerar: Ett år med datalagringen!” i Stadsnätet, Magasinet från Svenska stadsnätsföreningen, Nr 1 mars 2014.

[82] IT- och telekomföretagen, Arbetsgrupp för datalagring; Kalle Anrell och Monica Kleja, (22 november 2013) ”Stadsnäten stoppar överföringen”, Ny Teknik.

hetspolisens vilja och förväntan.[83]

Att trots mot ordningsmakten är det enda sättet att få reda på vad ordningsmakten gör, utgår vi ifrån inte är meningen. En viktig lärdom av historien är dock inte att en enskild teleoperatör sa ifrån, utan att den tekniska standardiseringen välkomnades av näringslivet. På grund av näringslivets redan befintliga förpliktelser, var det helt enkelt billigast och enklast för berörda företag att gå längre än man skulle.

Hur näringslivet kommer att anpassa sig till lagstiftarens önskemål går inte alltid lätt att förutse. Uppstår det juridisk osäkerhet kan det till exempel hända att utveckling mot bättre, användarvänliga säkerhetsverktyg inte kommer till stånd, snarare än att någon befintlig produkt försämras. Webbhotell, bloggplattformar, mediastationer och molntjänster tillhör sådana tjänster som kan tänkas påverkas av att det upplevs finnas ett krav på att kunna tillgängliggöra information till de brottsbekämpande myndigheterna. Om en sådan näringspolitisk utveckling ska ske, ska den inte ske för att utredare och lagstiftare inte haft möjlighet att överväga de näringspolitiska implikationerna av sina beslut.

Ur ett större och för utredningen mer allvarligt perspektiv, menar vi att svensk rättstradition är fast i en otidsenlig beskrivning av integritetsbegreppet som närmare motsvarar den gällande amerikanska lagstiftningen än den samtida europeiska, och som får både de brottsbekämpande myndigheterna och lagstiftarna att underskatta behovet av begränsningar för myndigheternas befogenheter med information om enskilda. Vi kommer att utveckla detta i det följande, men hänvisar också till vår behandling av ”vilda västern”-tendenser i elektroniska miljöer (se ovan sidan 3).

Incitament för kryptering och säkerhetsuppdateringar

Om beslag av information ska göras möjlig, är det viktigt att reglerna utformas på ett sådant sätt att de inte kräver avkryptering av krypterad information, samt att reglerna inte går att misstolka som ett incitament att inte låta konsumenter och enskilda själva ha makt över krypteringsnycklar.

Anledningen till detta är att man inte vill skapa incitament för näringslivet att frångå krypterade lösningar för sina slutanvändare. Man vill inte heller tvinga företag att implementera krypteringen på ett sådant sätt att företaget självt kan avkryptera informationen på begäran. Man vill alltså ha så kallad ”end-to-end-kryptering” där varje användare själv har eller kan ha kontroll över sina krypteringsnycklar.

Centraliserade lösningar, som att ha en huvudnyckel som låser upp alla elektroniska filer som lagrats på en viss dator, fungerar sämre och ger mindre säkerhet för konsumenter än decentraliserade lösningar som end-to-end-kryptering. Centraliserade lösningar är mer sårbara för både slarv (den vanligaste orsaken till säkerhetsproblem) och illasinnade attacker. Detta har observerats även i Sverige, då till exempel Försvarets radioanstalt har uttryckt oro inför användningen av molntjänster i offentlig sektor.[84]

Efter Snowden-läckorna har masskonsumentinriktade verksamheter som Wire, Google, Apple, Whatsapp, Telegram, Threema och Signal börjat använda

Se förklaring av Snowden-läckorna på sidan 17.

[83] P1 Morgon (17 december 2013) ”Bahnhof spelade in SÄPO:s övertalningskampanj”.

[84] Simon Camponello (12 februari 2016) ”FRA oroas av all outsourcing – vill att staten skapar eget moln”, IDG.

end-to-end-kryptering och starka dataskyddsfunktioner som en del av sin marknadsföring. Det har också uppstått en ”cryptoparty”-rörelse som plockats upp av, bland andra, svenska bibliotek.[85]

Denna utveckling är önskvärd och stärker enskildas och konsumenters förståelse och inflytande över sin egen säkerhet och identitet i digitala miljöer. Utvecklingen bör bejakas i rättspolitiken.

Figur 3: http://digibib.se/cryptoparty-bibldag16/

Överskottsinformation

Flera av uppgifterna i utredningsuppdraget berör möjligheten att samla in mer information vid husrannsakan, information om närstående, samt arkivering, gallring, kopiering och sekretess för sådan information.

Det är vår mening att utredaren bör föra Sverige närmare de tyska kontrollfunktionerna. Den tyska konstitutionsdomstolen var tidigt ute med att definiera ”informationellt självbestämmande”.[86] Senast våren 2016 etablerade domstolen att datorn effektivt är en förlängning av den enskilda individens personlighet.[87] Domstolen drar därför slutsatsen att övervakning av denna sfär är att ses som extra allvarlig och därför i de flesta fall därför omöjlig att rättfärdiga.

I Sverige berördes överskottsinformation så vitt vi har kunnat bedöma för första gången i utredningen Tvångsmedel – Anonymitet – Integritet från 1984.[88] Utredningen föreslog då att de brottsbekämpande myndigheterna inte skulle få använda överskottsinformation över huvud taget. Det förhållningssättet är förenligt både med det tyska konstitutionella skyddet, och det amerikanska konstitutionella skyddet. Den fria bevisprövningen i svenska domstolar har dock sedan 2003 inneburit att det inte finns några förhinder mot att brottsbekämpande myndigheter använder sig av bevisning i domstol som de i och för sig kommit

[85] Kungliga biblioteket (17 november 2015)”Bibliotekens behov av digitala miljöer med stöd för personlig integritet”

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

[87] Bundesverfassungsgericht, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 - Rn. (1-29) Paragraf 210:

> ”Mit dieser eigenständigen Ausprägung des allgemeinen Persönlichkeitsrechts trägt die Verfassung der heute weit in die Privatsphäre hineinreichenden Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung Rechnung (vgl. BVerfGE 120, 274 <302 ff.>). Tagebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens, Film- oder Tondokumente werden heute zunehmend in Dateiform angelegt, gespeichert und teilweise ausgetauscht. Weite Bereiche auch der höchstpersönlichen Kommunikation finden elektronisch mit Hilfe von Kommunikationsdiensten im Internet oder im Rahmen internetbasierter sozialer Netzwerke statt. Dabei befinden sich die Daten, auf deren Vertraulichkeit die Betroffenen angewiesen sind und auch vertrauen, in weitem Umfang nicht mehr nur auf eigenen informationstechnischen Systemen, sondern auf denen Dritter. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf diese Daten und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.”

[88] SOU 1984:54, Tvångsmedel - anonymitet - integritet.

över genom en process som inte är formellt riktig.[89] Detta bidrar till ett svenskt ”vilda västern” i digitala miljöer, vilket särskilt är fallet om de brottsbekämpande myndigheterna har långt gående befogenheter att bedriva underrättelsearbete, ta sig in i elektroniska system eller söka igenom datorer.

Nu är denna ”vilda västern”-stämning inte bara påkallad av att den svenska fria bevisprövningen – som enligt våra förslag bör begränsas – utan även av att svensk juristkår har en föråldrad inställning till integritet, privatliv och dataskydd. I utredningen om överskottsinformation vid direktåtkomst från 2012 drog utredningskommittéen inga andra slutsatser än att det behövs fler utredningar.[90] I utredningen om integritet och straffskydd beskrevs att svenska jurister uppfattar dataskyddslagstiftning som allt för svår, och att de inte har någon kunskap om lagstiftningen. Vi vill därför förtydliga några grundläggande aspekter av den europeiska dataskyddslagstiftningen, samt dess konceptuella ursprung.

Följande översikt av olika paradigmer för privatliv och integritet är tagen från Fahriye Seda Gürses avhandling i datavetenskap om integritetsskyddande teknologier (PETs).[91]

> 1870-talet: Rätten att bli lämnad i fred. (Integritet som hemlighet)
>
> En uppfattning om att det man vill hålla för sig själv, också ska hållas hemligt. Det som är privat, är privat, och ska inte lämna den privata sfären. Staten får i denna paradigm skyldigheten att inte avhända sina subjekt mer information än nödvändigt, för om staten gör det antas informationen ha hamnat utanför subjektets kontroll och därmed inte längre vara privat. Det är denna syn som i princip är inbakad i svenska regeringsformen.
>
> 1970-talet: Rätten till dataskydd. (Integritet som kontroll)
>
> I detta paradigm antar man istället att subjektet kan utöva kontroll över uppgifter även som gjorts tillgängliga för andra. Istället för att man tappar kontrollen, kan man få möjlighet till rättelse, insyn, och en möjlighet att säga nej till fortsatt behandling. De första dataskyddslagstiftningarna är skrivna mot bakgrund av detta nya paradigm, och den europeiska dataskyddslagstiftningen håller sig även efter den politiska processen att ta fram en ny allmän dataskyddsförordningen huvudsakligen inom detta paradigm.
>
> 2000-talet: Rätten till en egen identitet. (Integritet som praktik)
>
> Detta paradigm har påverkats av rättsutvecklingen i tyska konstitutionsdomstolen och Europadomstolen, och innebär att individer utöver de verktyg som finns i dataskyddslagstiftning och som härstammar ur det andra paradigmet ska ha en rätt att själva utveckla sin identitet utan otillbörlig påverkan utifrån. Synsättet flyttar tonvikten från uppgifter som direkt går att härleda till ett subjekt, till de mer abstrakta mängderna av information som rör ett subjekts identitet.

Det sista synsättet kan anses ha representerats i utredningen om en ny da-

[89] Högsta domstolen, NJA 2003 s. 323.
[90] SOU 2012:90, Överskottsinformation vid direktåtkomst.
[91] Fahriye Seda Gürses, ”Multilateral Privacy Requirements Analysis in Online Social Network Services” KU Leuven, 2010.

talag från 1993,[92] men föll på att domstolarna inte upplevde att de kunde göra adekvata bedömningar från fall till fall.

I Sverige har domstolsväsendet ofta haft en tillbakadragen roll, enligt Johansen och Wejedal så pass tillbakadragen att mycket litet har skiljt domstolarna från vanliga förvaltningsmyndigheter,[93] vilket skapar dåliga förutsättningar för en flexibel lagstiftning där individer genom att tilldelas information själva kan driva klagomål och be domstolarna om tvistlösning även i situationer som lagstiftaren inte direkt har förutsett. Problemet kan antas vara kopplat till den konsumenträttsliga problem vi har anfört på sidan 7 om möjligheter för enskilda att hävda sin rätt.

Trots enstaka nedslag i mer moderna tillvägagångssätt för att hantera rätten till integritet (rätten till identitet) har den svenska lagstiftningen huvudsakligen gått tillbaka till en syn på integritet som motsvarar 1870-talsbegreppet. I vilket fall saknas det både doktrin och statliga utredningar som tar avstamp i rätten till privatliv och integritet som en rätt till den egna identiten, innefattat den identitet eller de identiteter man utvecklat med och genom elektroniska verktyg.

Istället för att bemäktiga privatpersoner att få kunskap och kännedom om hur de påverkas av andra, har lagstiftaren arbetat med en dataskyddsprincip som de kallar för ”missbruksregeln”. Den har inspirerats av amerikansk lagstiftning och så vitt Dataskydd.net kunnat utröna finns det inga utredningar om huruvida missbruksregeln alls har förutsättningar att upprätthållas i Sverige: till skillnad från USA saknar nämligen Sverige en utvecklad skadeståndsrätt och svenska domstolar har inte möjlighet, eller befogenhet, att ägna sig åt samma fria konfliktlösning som amerikanska domstolar.[94]

I den amerikanska doktrinen (som förvisso är stor och därför spretigare än den svenska) har man rört sig åt motsatt håll från den svenska. Framstående forskare som Helen Nissenbaum[95] och Bruce Schneier[96] förespråkar en europeiskinspirerad hanteringsmodell för dataskydd, och den avgående presidenten Barack Obama har initierat en process för moderna regler för dataskydd.[97]

De svenska reglerna om hantering av överskottsinformation, men även hantering av personuppgifter i staten i allmänhet, har uppstått utanför den här kontexten. I Sverige görs därför ingen stark åtskillnad mellan de enskildas intressen och de statliga intressena. ”Det allmänna” och ”allmänheten” verkar inte ses som separata aktörer med olika intressen. Eftersom ”allmänheten” består av en brokig skara enskilda, naturliga personer, har konsekvensen av denna brist på åtskillnad mellan ”det allmänna” och ”allmänheten” blivit att ”det allmännas” intressen övertar ”allmänhetens” intresse. Allmänheten har helt enkelt sämre politiska verktyg att göra sig hörda än vad förvaltningsväsendet har (och förvaltningsväsendet kan i detta tillmätas en vidare betydelse än bara de brottsbekämpande myndigheterna). Markus Naarttajärvi berör någonting liknande i sin avhandling från 2013, dock utan att göra en så tydlig och långtgående

[92] SOU 1993:10, En ny datalag
[93] Se ovan fotnot 4.
[94] Dataskydd.net, Remissyttrande över SOU 2016:7 om integritet och straffskydd, maj 2016.
[95] Helen Nissenbaum, ”Must Privacy Give Way to Use Regulation?” Brown University Watson Event, 15 mars 2016.
[96] Bruce Schneier, ”Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World”, W. W. Norton & Company, 2015.
[97] Vita huset, ”We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consumers Online”, 23 februari 2012.

slutsats.[98]

Genom att omdefiniera rätten till integritet från att vara ett skydd för enskildas självständiga personlighetsutveckling till någonting som ger staten rätt att utreda brottslig verksamhet,[99] avviker svensk rättsutveckling från den utveckling av integritets- och identitetsbegreppet som ägt rum i Europa och i världen i övrigt. Utredaren bör bryta denna trend och istället lyfta fram allmänhetens intresse av att varje enskild individ kan utöva självständigt inflytande över sin identitetsbildning i så hög utsträckning som är rimligt.

Vårt förslag är att man begränsar tillämpningen av hemliga tvångsmedel på ett sådant sätt att bara sådan information som angivits i tillståndet för tillämpningen av det hemliga tvångsmedlet får samlas in. En sådan avgränsning har stöd i tysk rätt, och även i amerikansk, och vore en tillbakagång till de egentligen mer moderna resonemang om rätten till privatliv och identitet som i Sverige fördes på 1970- och 80-talen.

I övrigt är vi negativa till de saker som lyfts i utredningsuppdraget och som innebär att brottsbekämpande myndigheter får större befogenheter att inskränka inte bara vagt misstänkta individers privata sfär, utan även deras anhörigas och vänners privata sfärer. Privatpersoner i Sverige är människor och åtnjuter därigenom rätten till en egen identitet. Tvångsåtgärder ska vara specifika, riktade, avgränsade och förutsägbara för de som drabbas.

Förslag

1. En regel om att det som inte är tillåtet inte ska göras av de brottsbekämpande myndigheterna

Vi efterfrågar en regel om att det som inte är reglerat i lag, inte ska vara tillåtet för myndigheterna att göra. En sådan regel är överensstämmande med de internationella förpliktelser som Sverige är bundna av med avseende på rättssäkerhet och förutsägbarhet för myndigheters handlingar.

Se ovan sidan 3, 15, 20.

2. Konsumenter bör kunna förvänta sig att deras stat upprätthåller antingen juridisk säkerhet eller möjligheter för teknisk säkerhet.

Ett nytt förfarande för husrannsakan som innebär att de brottsbekämpande myndigheterna kan riskera att bevara tekniska säkerhetsfel (sårbarheter) eller agera för att sårbarheter inte ska åtgärdas försämrar konsumenternas tekniska säkerhet. Om utredaren vill införa ett sådant förfarande, bör utredaren föreslå stärka konsumenternas juridiska säkerhet i enlighet med Fördraget om Europeiska unionens funktionssätt (2012/C 326/01) artikel 169(4), så att risken och bevisbördan för att en elektronisk signatur är äkta inte faller på konsumenten. Även vid sådana transaktioner som inte innefattar elektroniska signaturer bör bevisbördan flyttas från konsumenten till tjänsteleverantören/erna.

Se ovan sidorna 4, 5, 7.

98 Se ovan fotnot 45.
99 Cecilia Gustavsson (4 april 2001) ”Storebror ser dig och följer dig hem”.

3. Det ska ställas starka krav på rättssäkerhet i form av oberoende förhandsprövning av metoden för husrannsakan samt möjlighet till efterhandsgranskning.

Den oberoende instans som genomför förhandsprövningen måste få tillgång till tillräckligt med information för att fatta ett informerat beslut i enlighet med Europadomstolens praxis för oberoende prövningar. Informationen ska innefatta en redovisning av hur myndigheterna tekniskt kommer att genomföra och avsluta husrannsakan. Den ska också innefatta vad myndigheterna letar efter och hur de ska undvika att lägga beslag på sådant de inte letar efter. Dessa regler ska gälla både då myndigheterna undersöker elektronisk apparatur de befinner sig i fysisk närhet av (genomsökning av elektronisk apparatur) eller om de genomför ett sanktionerat dataintrång.

Se ovan sidorna 3, 13, 20.

4. De brottsbekämpande myndigheterna ska offentligt och lättillgängligt redovisa de metoder de har använt för att utnyttja sårbarheter i programvaror och andra elektroniska system.

Oavsett om de brottsbekämpande myndigheternas har fått tag på metoderna för att utnyttja sårbarheter från andra myndigheter eller från näringslivet ska användningen omfattas av en redovisningsplikt som ska göras offentlig. Det ska alltså inte vara möjligt för myndigheterna att begagna sig av en metod för att utnyttja en sårbarhet i programvaror eller elektroniska system upprepade gånger utan att sårbarheten sedan kan åtgärdas. Det behöver tydligt framgå att myndigheterna inte ska kunna vända sig till andra myndigheter med starkare sekretesskydd för att kringgå dessa förpliktelser. Det ska heller inte vara möjligt att undgå transparenskraven genom hänvisning till företagshemligheter i privat sektor.

Se ovan sidorna 11, 13.

5. De brottsbekämpande myndigheterna ska ha ett strikt ansvar för att deras metoder att ta sig in i system på distans når de personer de är menade att nå.

Ansvaret för att en sårbarhet som utnyttjats i en programvara eller annat elektroniskt system i enlighet med lagen inte hamnar på villovägar, till exempel smittar andra system än det som är avsett i tillståndet, ska vara strikt. För att det ska finnas en möjlighet att utkräva ett sådant ansvar måste transparensförpliktelserna i förslag 3 och 4 realiseras.

Se ovan sidorna 4–, 13, 15.

6. Tidigare okända sårbarheter eller metoder för att utnyttja sårbarheter (0-days) ska inte användas vid sanktionerade dataintrång utan omedelbart meddelas den näringslivsaktör eller annan aktör som bäst kan åtgärda dem.	
Om de brottsbekämpande myndigheterna får kännedom om en tidigare okänd sårbarhet eller metod för att utnyttja en sårbarhet ska de omedelbart vidta åtgärder för att sårbarheten eller metoden att använda sårbarheten blir känd och kan åtgärdas.	Se ovan sidan 13.
7. En särskild regel om att de brottsbekämpande myndigheterna inte ska få efterfråga svagare säkerhet än vad som är tekniskt möjligt.	
Sverige bör införa en särskild regel om att myndigheter inte ska göra konsumenters och privatpersoners liv otryggare i elektroniska miljöer än vad som av ekonomiska skäl är oundvikligt.	Se ovan sidan 12.
8. Den fria bevisprövningen bör avgränsas på ett sådant sätt att de brottsbekämpande myndigheterna inte har operativa incitament att leta efter och spara mer information än de fått tillstånd att leta efter och spara från domstol.	
Användning av hemliga tvångsmedel ska vara avgränsad och specifikt och tillägnad särskilda målsättningar. Sådan information som inte ingår i underlaget för användningen av det hemliga tvångsmedlet ska inte kunna användas vid rättegångar, det ska inte sparas, lagras, kopieras eller på annat sätt behandlas av myndigheten. Svensk lagstiftning behöver en särskild regel som skyddar enskilda mot fiskeexpeditioner under förundersökningar och underrättelsearbete.	Se ovan sidan 20.

Källhänvisningar med länkar där möjligt

Akademi

1. Ross Anderson. ”Why Cryptosystems Fail” ACM. 1st Conf. - Computer and Communication Security 1993. http://www.cl.cam.ac.uk/users/rja14/wcf.html
2. Axel M. Arnbak. ”Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives” doktorsavhandling, Universiteit van Amsterdam, 2015. http://dare.uva.nl/record/1/492674
3. Steven M. Bellovin, Matt Blaze, Sandy Clark, Susan Landau, ”Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet”. Privacy Legal Scholars Conference, June 2013. http://ssrn.com/abstract=2312107
4. Henrik Bengtsson, advokat, Advokatfirman Delphi, datum okänt, ”Bevisbörda och beviskrav vid invändning om underskriftsförfalskning – särskilt om elektroniska signaturer”. http://delphi.se/$-1/file/artiklar/2013/bevisborda-och-beviskrav-vid-invandning-om-underskriftsforfalskning-sarskilt-om-elektroniska-signaturer-i-kihlman-ed-elektroniska-signaturer-henrik-bengtsson.pdf
5. Jean-Francois Blanchette, ”Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents” MIT Press, 2012

6. Nicholas Bohm et al, ”Electronic Commerce: Who Carries the Risk of Fraud?” 2000 (3) The Journal of Information, Law and Technology (JILT) http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/
7. CitizenLab Publications. https://citizenlab.org/publications/
8. Jennie Grön. ”Framtidens bok – från avtalat ägande till övervakat lån” Examensarbete i civilrätt. Juridiska fakulteten, Uppsala universitet, 2015. http://uu.diva-portal.org/smash/get/diva2:811095/FULLTEXT04.pdf
9. Fahriye Seda Gürses, ”Multilateral Privacy Requirements Analysis in Online Social Network Services” KU Leuven, 2010. https://www.cosic.esat.kuleuven.be/publications/thesis-177.pdf
10. Pierre Halsius, ”Nationella insatsstyrkan - nutid och framtid”, Rapport 399 vid Polisutbildningen vid Umeå universitet, vårterminen 2007 http://www.diva-portal.se/smash/get/diva2:276599/FULLTEXT01.pdf
11. Tormod Otter Johansen och Sebastian Wejedal, ”Mot ett funktionellt domstolsbegrepp – Ett bidrag med anledning av den så kallade Försvarsunderrättelsedomstolen”, SvJT 2016 s. 10 res 191
12. Lennart Johansson, ”Banker och internet” Iustus förlag (Stockholm), 2006.
13. Stefan Larsson och Per Runesson (ed), ”Digitrust: Tillit i det digitala” Lunds universitet juni 2014. http://digitalsociety.se/2014/06/11/ny-rapport-tillit-i-det-digitala/
14. Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “For Their Eyes Only: The Commercialization of Digital Spying,” Citizen Lab Research Brief No. 17, April 2013. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf
15. Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “You Only Click Twice: FinFisher’s Global Proliferation,” Citizen Lab Research Brief No. 15, March 2013. https://citizenlab.org/wp-content/uploads/2009/10/You-Only-Click-Twice-FinFisher%E2%80%99s-Global-Proliferation.pdf
16. Morgan Marquis-Boire (lead technical research) and Jakub Dalek (lead technical research), Sarah McKune (lead legal research), Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman, “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,” Citizen Lab Research Brief No. 13, January 2013. https://citizenlab.org/wp-content/uploads/2015/03/Planet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-ToolsPlanet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-Tools.pdf
17. Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, ”Chip and PIN is Broken” 2010 IEEE Symposium on Security and Privacy. https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf
18. Markus Naarttijärvi. Doktorsavhandling, Umeå universitet, 2013. ”För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel” http://umu.diva-portal.org/smash/record.jsf?pid=diva2%3A664052&dswid=-3145
19. Helen Nissenbaum, ”Must Privacy Give Way to Use Regulation?” Brown University Watson Event, 15 mars 2016. http://watson.brown.edu/events/2016/helen-nissenbaum-must-privacy-give-way-use-regulation
20. Karin Nygren, ”Problemorienterat polisarbete”, Rapport 472 vid Polisutbildningen vid Umeå universitet http://umu.diva-portal.org/smash/get/diva2:276671/FULLTEXT01.pdf
21. Stephanie K Pell, Christopher Soghoian. ”Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy” Harvard Journal of Law and Technology, Volume 28, Number 1 Fall 2014 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678
22. Bruce Schneier, ”Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World”, W. W. Norton & Company, 2015.

Offentliga institutioner

1. Council of Europe, Recommendation (89) 9 on computer-related crime and and final report of the European Committee of Crime Problems (1989) http://www.oas.org/juridico/english/89-9&finalReport.pdf
2. Council of Europe, Parliamentary Assembly, Resolution 2045 (2015) ”Mass surveillance” Text adopted by the Assembly on 21 April 2015 (12th Sitting), med tillhörande Recommendation 2067 (2015). http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en
3. EDPS, Opinion 8/2015: Dissemination and use of intrusive surveillance technologies. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-12-15_Intrusive_surveillance_EN.pdf
4. EU-kommissionen (2006). COM (2006) 744 final. Green Paper on the Review of the Consumer Acquis. http://ec.europa.eu/consumers/archive/cons_int/safe_shop/acquis/green-paper_cons_acquis_en.pdf
5. EU-kommissionen (2007) Detailed analysis of responses to the European Commission Green Paper on Consumer Rights Reform http://ec.europa.eu/consumers/archive/rights/detailed_analysis_en.pdf
6. EU-kommissionen (2015). Public consultation on contract rules for online purchases of digital content and tangible goods. http://ec.europa.eu/justice/newsroom/contract/opinion/150609_en.htm
7. EU-kommissionen (2015) COM (2015) 634 final. Förslag till Europaparlamentets och rådets direktivet om vissa aspekter på avtal om tillhandahållande av digitalt innehåll. http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52015PC0634&from=EN
8. Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32014R0910&from=EN
9. Europol, Director’s Speech at the conference: Privacy in the Digital Age of Encryption and Anonymity Online, Haag, Nederländerna, 19 maj 2016. https://www.europol.europa.eu/node/4604
10. Nederlandse overheid, Ministerie van Defensie, ”Gegevens verwerken met ARGO II” https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/inhoud/inlichtingen-en-veiligheid/gegevens-verwerken-met-argo-ii
11. Kungliga biblioteket (17 november 2015) ”Bibliotekens behov av digitala miljöer med stöd för personlig integritet” https://biblioteksamverkan.blogg.kb.se/2015/11/17/bibliotekens-behov-av-digitala-miljoer-med-stod-for-personlig-integritet/
12. Post- och telestyrelsen. Strategi för ett säkrare Internet i Sverige. PTS-ER-2006:12. https://www.pts.se/sv/Dokument/Rapporter/Internet/2006/Strategi-for-ett-sakrare-Internet-i-Sverige---PTS-ER-200612/
13. SOU 1972:47, Data och integritet http://weburn.kb.se/metadata/729/SOU_8350729.htm
14. SOU 1984:54, Tvångsmedel - anonymitet - integritet http://weburn.kb.se/metadata/933/SOU_7261933.htm
15. SOU 1993:10, En ny datalag http://weburn.kb.se/metadata/201/SOU_8351201.htm
16. SOU 2006:98, Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2006/11/sou-200698/
17. SOU 2007:76. Lagring av trafikuppgifter för brottsbekämpning. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/11/sou-200776/
18. SOU 2012:90, Överskottsinformation vid direktåtkomst. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/01/sou-201290/
19. SOU 2013:39, Europarådets konvention om it-relaterad brottslighet. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/06/sou-201339/

20. United States Department of Commerce, National Telecommunications and Information Administration, ”Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities”, 13 maj 2016. https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

21. Vita huset, Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, 12 december 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

22. Vita huset, ”We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consumers 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

Nyhetsartiklar

1. Nate Anderson (11 mars 2013)”The Remote Administration Tool is the revolver of the Internet’s Wild West”, Ars Technica. http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/

2. Kalle Anrell och Monica Kleja, (22 november 2013) ”Stadsnäten stoppar överföringen”, Ny Teknik. http://www.nyteknik.se/digitalisering/stadsnaten-stoppar-direktoverforingen-6401476

3. John Bakke (12 juni 2015). ”Polis ville hacka Facebook” SVT. http://www.svt.se/nyheter/lokalt/vasterbotten/polisen-bad-om-hjalp-att-hacka-facebook

4. Jan Bertoft (29 april 2015) ”Se upp för Blocket”, Egen blogg för ordföranden i Sveriges konsumenter. http://bertoft.se/2015/04/se-upp-for-blocket/

5. Bloomborg (30 mars 2016) ”FBI Worked With Israel’s Cellebrite to Crack iPhone” http://www.bloomberg.com/news/articles/2016-03-30/fbi-said-to-work-with-israel-s-cellebrite-to-crack-iphone

6. Blåljus.nu (20 oktober 2011) ”Hur skulle svenska polischefer klara möte med ”CompStat”?” http://www.blaljus.nu/nyhetsartikel/hur-skulle-svenska-polischefer-klara-mote-med-compstat

7. Blåljus.nu (30 juni 2015) ”Framtidens polis i förorten”. http://www.blaljus.nu/nyhetsartikel/framtidens-polis-i-fororten

8. Tobias Brandel (19 februari 2014) ”USA dominerar skev världsbild i riksdagen” Svenska dagbladet. http://www.svd.se/usa-dominerar-skev-varldsbild-i-riksdagen

9. Sara L Bränström (4 mars 2016) ”Riksbanken: Då blir Sverige kontantlöst”, Svenska dagbladet. http://www.svd.se/riksbanken-da-blir-sverige-kontantlost

10. Stuart Burns (20 maj 2016) ”Hacked in a public space? Thanks, HTTPS”, The Register. http://www.theregister.co.uk/2016/05/20/https_wifi_trust_in_a_public_place/

11. Simon Camponello (12 februari 2016) ”FRA oroas av all outsourcing – vill att staten skapar eget moln”, IDG. http://computersweden.idg.se/2.2683/1.650026/fra-staten-moln

12. Mike Carter (27 oktober 2014) ”FBI created fake Seattle Times Web page to nab bomb-threat suspect”, Seattle Times http://www.seattletimes.com/seattle-news/fbi-created-fake-seattle-times-web-page-to-nab-bomb-threat-suspect/

13. Guillaume Champeau (13 januari 2016) ”Chiffrement : le gouvernement rejette les backdoors”, Numerama. http://www.numerama.com/politique/138689-chiffrement-le-gouvernement-rejette-les-backdoors.html

14. Graham Cluley (10 oktober 2011) ”German ‘Government’ R2D2 Trojan FAQ”, Naked Security (Sophos) https://nakedsecurity.sophos.com/2011/10/10/german-government-r2d2-trojan-faq/

15. Joseph Cox (6 juli 2015) ”The FBI Spent $775K on Hacking Team’s Spy Tools Since 2011”, Wired https://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/

16. Dataskydd.net, (15 maj 2016) ”Lågt skydd för konsumenter som vill stärka sin säkerhet” https://dataskydd.net/lagt-skydd-konsumenter-som-vill-starka-sin-sakerhet

17. Mattias Frödén (23 april 2016) ”Härvan växer - hundratals offer för pizzabluffen”, Nerikes allehanda. http://na.se/nyheter/orebro/1.3793193-harvan-vaxer-hundratals-offer-for-pizzabluffen

18. Ryan Gallagher (1 november 2011) ”Governments turn to hacking techniques for surveillance of citizens” The Guardian. https://www.theguardian.com/technology/2011/nov/01/governments-hacking-techniques-surveillance

19. Andy Greenberg (21 March 2012). ”Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)” Forbes. http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/#b84a4e094483

20. Cecilia Gustavsson (4 april 2001) ”Storebror ser dig och följer dig hem”. http://www.aftonbladet.se/wendela/article10204441.ab

21. Adrianne Jeffries (13 September 2013). ”Meet Hacking Team, the company that helps the police hack you” The Verge. http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers

22. Matthijs R. Koot (5 januari 2016). ”Full translation of the Dutch government’s statement on encryption” Cyberwar. https://blog.cyberwar.nl/2016/01/full-translation-of-the-dutch-governments-statement-on-encryption/

23. Linus Larsson (28 januari 2015) ”Så spanar polisen på Facebook” Dagens nyheter. http://www.dn.se/ekonomi/sa-spanar-polisen-pa-facebook/

24. Lotta Lille (12 oktober 2012) ”Bedragare stal semesterkassan”, Upsala nya tidning. http://www.unt.se/uppland/heby/bedragare-stal-semesterkassan-1900975.aspx

25. Doug Olenick (8 februari 2016) ”Skype targeted by T9000 backdoor trojan”, SCMagazine http://www.scmagazine.com/skype-targeted-by-t9000-backdoor-trojan/article/471958/

26. Philip Oltermann (8 februari 2016) ”German plan to impose limit on cash transactions met with fierce resistance”, The Guardian. http://www.theguardian.com/world/2016/feb/08/german-plan-prohibit-large-5000-cash-transactions-fierce-resistance

27. P1 Morgon (17 december 2013) Bahnhof spelade in SÄPO:s övertalningskampanj https://sverigesradio.se/sida/artikel.aspx?programid=1650&artikel=5735355

28. P1 Plånboken (30 mars 2016) https://sverigesradio.se/sida/avsnitt/698348?programid=2778

29. Michael Persson (9 november 2013) ”Nederland bestelt een nog verboden spionagesysteem”, Volkskrant http://www.volkskrant.nl/tech/nederland-bestelt-een-nog-verboden-spionagesysteem~a3541591/

30. Peter Pi (7 juli 2015) ”Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak”, Trendlabs Security Intelligence Blogs. http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/

31. Bruce Schneier (25 februari 2011) ”HBGary and the Future of the IT Security Industry”, schneier.com https://www.schneier.com/blog/archives/2011/02/hbgary_and_the.html

32. Vernon Silver (8 november 2012) ”MJM as Personified Evil Says Spyware Saves Lives Not Kills Them” Bloomberg. http://www.bloomberg.com/news/articles/2012-11-08/mjm-as-personified-evil-says-spyware-saves-lives-not-kills-them

33. Der Spiegel, 9 november 2014 ”BND will Informationen ueber Software-Sicherheitsluecken einkaufen” http://www.spiegel.de/spiegel/vorab/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001771.html

34. Spielerecht.de, Osborne Clarke Publication number 1506540 ”Update: Valve May Prohibit Steam Account Transfers – German Judgment” mars 2014 http://spielerecht.de/wp-content/uploads/Update_-Valve-May-Prohibit-Steam-Account-Transfers-German-Judgment-Published.pdf

35. Svenska dagbladet (12 februari 2015) ”Anders Ygeman till terrormöte i USA” http://www.svd.se/anders-ygeman-till-terrormote-i-usa

36. Craig Timberg och Ellen Nakashima (6 december 2013) ”FBI’s search for ‘Mo,’ suspect in bomb threats, highlights use of malware for surveillance”, Washington Post https://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html

37. Tronarp, Ornerud, Hagberg (18 augusti 2015) ”Högsta domstolen stoppar husrannsakan på Aftonbladet”, Aftonbladet. http://www.aftonbladet.se/nyheter/article21270168.ab

38. Verbraucherzentrale Bundesverband. (6 juni 2013). ”Samsung App-Store: Viele Klauseln unzulässig.” http://www.vzbv.de/urteil/samsung-app-store-viele-klauseln-unzulaessig

39. Kim Zetter (31 augusti 2009) ”Code for Skype Spyware Released to Thwart Surveillance”, Wired https://www.wired.com/2009/08/skype-trojan/

40. Geronimo Åkerlund (21 januari 2016) ”Därför pixlar vi”, SVT. http://www.svt.se/nyheter/lokalt/stockholm/darfor-pixlar-vi

41. Kristoffer Örstadius (28 oktober 2014) ”Vanliga modem lätta att kapa”, Dagens nyheter http://www.dn.se/ekonomi/vanliga-modem-latta-att-kapa/

Rättsfall

1. Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1. Domen finns inte tillgänglig på Bundesverfassungsgerichts hemsida, men finns här: http://www.servat.unibe.ch/dfr/bv065001.html#.

2. Bundesverfassungsgericht, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007.html

3. Bundesverfassungsgericht, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 - Rn. (1-29), http://www.bverfg.de/e/rs20160420_1bvr096609.html

4. Europadomstolen, Zakharov v. Russia (Application no. 47143/ 06). http://hudoc.echr.coe.int/eng?i=001-159324

5. Europadomstolen, Szabo och Vissy v Hungary (Application no. 37138/14). http://hudoc.echr.coe.int/eng?i=001-160020

6. Högsta domstolen, NJA 2003 s. 323. https://lagen.nu/dom/nja/2003s323

Övrigt (opinionsundersökningar och dylikt)

1. Dataskydd.net, Remissyttrande över SOU 2016:7 om integritet och straffskydd, maj 2016. https://dataskydd.net/sites/default/files/dataskyddnet_remissyttrande_sou201607_20160509.pdf

2. 2016 CIGI-Ipsos Global Survey on Internet Security and Trust https://www.cigionline.org/internet-survey-2016

3. Internetstiftelsen i samarbete med Insight Intelligence och SICS samt svenska näringslivsaktörer och Stockholms landsting, Delade meningar 2, mars 2016. https://www.iis.se/docs/Delade-Meningar-2016.pdf

4. IT- och telekomföretagen, Arbetsgrupp för datalagring. https://www.itotelekomforetagen.se/fakta-och-debatt/nyheter-och-aktuellt/aktuellt-arkiv/arbetsgrupp-trafikdatalagring

5. Tor Borrhed, ”Maintrac summerar: Ett år med datalagringen!” i Stadsnätet, Magasinet från Svenska stadsnätsföreningen, Nr 1 mars 2014. http://www.ssnf.org/globalassets/nyheter/stadsnatsmagasinet/sn_1_2014.pdf