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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Chicago 2018-03-06

Remissyttrande över utredningen om hemlig dataavläsning – SOU 2017:89 (Ju2017/08898/Å)

Redaktör: Amelia Andersdotter.
Bildredaktör: Karolina Rediviva.
LaTeX: Anders Jensen-Urstad / tufte-latex.

Totalt föreslår vi 10 ändringar, och återproducerar i två därpå följande stycken vissa resonemang vi tidigare anfört om datasäkerhet och informationssäkerhet för enskilda. I ett sista avsnitt bemöter vi utredarens avfärdanden av våra krav på insyn i och redovisning av de brottsbekämpande myndigheter verkställighetsmetoder.

Innehållsförteckning:

Sammanfattning

Det räcker inte att proportionaliteten i sanktionerade dataintrång[1] bedöms i statliga utredningar. Proportionaliteten behöver kontinuerligt bedömas inför varje enskild tillämpning av tvångsmedlet. Redovisning av åtgärder inom ramen för aktsamhetskravet som utredaren föreslagit i 20§ bör utgöra en del av *legalkraven* för att alls få använda tvångsmedlen, för att förebygga slarv och hot mot enskildas och samhällets informationssäkerhet. Se våra föreslagna ändringar i 3 § och 13 §.

Förteckningen av de brott för vilka tvångsmedlet ska kunna appliceras bör vara uttömmande i lagen, och motsvaras av det behov utredaren påvisat. Regeringens fortsatta arbete att skärpa straffskalor inom en rad områden innebär nämligen annars att varje annan form av brott eventuellt kan förorda sanktionerade dataintrång. Därtill är det otillfredsställande att en massa *icke misstänkta individer* ska kunna hackas av åklagare, polis och Säkerhetspolis, bara *utifall att*

[1] Se avsnitt *Åtgärder som försämrar informationssäkerhet för enskilda och konsumenter* (avsnitt) för definitioner.

de skulle behöva misstänkas. Se våra föreslagna ändringar i 4 §, men även 6-10 §§, samt därpå följande ändringar i 24–28 §§.

Sverige har redan tidigare hamnat i blåsvädret, bland annat genom Tele2-målet i EU-domstolen, för den frihetliga inställningen till föregående, oberoende prövning. När de brottsbekämpande myndigheternas frihet att okontrollerat agera kolliderar med medborgarnas rättighet att förutse vad de brottsbekämpande myndigheterna kan ta sig till, bör den senare rättigheten enligt Dataskydd.net och även de människorättskonventioner Sverige förbundit sig att upprätthålla ges företräde. Interimistiska prövningar bör alltså inte tillåtas. Se vår föreslagna ändring i 13–14 §§.

I ett utvärderingsskede bör man inte heller tillåta någon insamling av överskottsinformation. Utredarens förslag på området (se kap. 10.11.2 i utredningen) motsvaras inte av något demonstrerat behov, utan förefaller ha tillkommit "bara för att det alltid funkat så". Men prostitution är ett gammalt yrke och länge fick man slå sin fru – det har inte hindrat lagstiftaren från att skapa nya bättre lösningar för en modern tid, och likadant bör regeringskansliet resonera kring överskottsinformation. Att reglerna tidigare varit dåliga är inget skäl att de ska fortsätta vara dåliga. Se vår förslagna ändring 23 § och följdändringar i 26–27 §§.

Förslag

ÄNDRING 1

Utredarens förslag Lag om hemlig dataavläsning, 2 §	Dataskydd.net:s förslag Lag om hemlig dataavläsning, 2 §
Ett tillstånd till hemlig dataavläsning får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.	Ett tillstånd till hemlig dataavläsning får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse. Till grund för bedömningen om tillståndets lagenlighet ska särskilt ligga den aktsamhet enligt 20 § i denna lag som utförande myndigheter.

SKÄL: I utredarens förslag är aktsamhetskravet i 20 § hängande: en aspiration eller förhoppning om att det ska finnas en plan om något går fel, men utan tillstymmelse till försök att garantera att en sådan finns eller att behovet av den ens har förutsetts. Eftersom utredaren själv observerar att hennes förslag kan leda till allvarliga konsekvenser för informationssäkerheten för privatpersoner, privata företag och samhället i stort synes det nödvändigt att man redan vid tillståndsprövningen har en plan för hur skadliga effekter ska minimeras.

ÄNDRING 2

Utredarens förslag

Lag om hemlig dataavläsning, 4 §

Hemlig dataavläsning får, om inte annat anges i andra eller tredje stycket, användas vid en förundersökning om ~~brott som anges i 27 kap. 18 § andra stycket rättegångsbalken~~ om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. En åtgärd enligt 2 § första stycket 4 får användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

~~Hemlig dataavläsning enligt 2 § första stycket 2 och 3 får också användas för att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Om åtgärden innebär att uppgifter om meddelanden enligt 2 § första stycket 2 läses av eller tas upp får uppgifterna dock endast avse förfluten tid.~~

Hemlig dataavläsning enligt 2 § första stycket 5 får endast användas vid en förundersökning om ~~brott som anges i 27 kap. 20 d § andra stycket rättegångsbalken~~ om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Är platsen någon annan stadigvarande bostad än den misstänktes, får hemlig dataavläsning enligt 2 § första stycket 5 användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. På en plats som anges i 12 § tredje stycket får hemlig dataavläsning enligt 2 § första stycket 5 aldrig användas.

Dataskydd.net:s förslag

Lag om hemlig dataavläsning, 4 §

Hemlig dataavläsning får, om inte annat anges i andra eller tredje stycket, användas vid en förundersökning om *barnpornografibrott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, grovt spionerienligt 19 kap. 6 § brottsbalken, grovt sabotage enligt 13 kap. 5 § brottsbalken, samt terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant terroristbrott om det med hänsyn till omständigheterna kan antas att gärningens straffvärde överstiger fängelse i fyra år, och* om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. En åtgärd enligt 2 § första stycket 4 får användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Hemlig dataavläsning enligt 2 § första stycket 5 får endast användas vid en förundersökning om *dataintrång enligt 4 kap. 9 c § brottsbalken, människohandel enligt 4 kap. 1 a § brottsbalken, grovt sexuellt tvång enligt 6 kap. 2 § tredje stycket brottsbalken, våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken, grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken, spionerienligt 19 kap. 5 § brottsbalken, samt försök, förberedelse eller stämpling till sådana brott om det med hänsyn till omständigheterna kan antas att gärningens straffvärde överstiger fängelse i fyra år, och* om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Är platsen någon annan stadigvarande bostad än den misstänktes, får hemlig dataavläsning enligt 2 § första stycket 5 användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. På en plats som anges i 12 § tredje stycket får hemlig dataavläsning enligt 2 § första stycket 5 aldrig användas.

SKÄL: Förteckningen av brott för vilka tvångsmedlet aktualiseras bör vara uttömmande, och är i det här fallet ihopsnickrad efter Dataskydd.net förståelse av de situationer där polismyndigheten uppgivit att de vill använda tvångsmedlet i utredningens kapitel 7, utredarens förslag i Lag om hemlig dataavläsning 8 § samt de tidigare hänvisade artiklarna i rättegångsbalken (som dock är betydligt bredare i omfattning än vad Dataskydd.net:s listor, som ju är behovsprövade utifrån utredarens utredning, är).
Andra stycket i utredarens förslag är oortodoxt och osunt. Allvarligt tunga tvångsmedel ska inte kunna användas mot människor som *inte är misstänkta för brott*. Vad förslaget innebär är i praktiken att *alla medborgare alltid* lider en risk att få sin informationssäkerhet nedsatt eller förstörd av polisiära åtgärder, vilket är mycket olämpligt i dessa tider av ökande identitetsstöld, fler och fler betalningsbedrägerier, välfärdsbedrägerier, och dylikt.

ÄNDRING 3

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 6-10 §§	Lag om hemlig dataavläsning, 6-10 §§
~~Hemlig dataavläsning utanför en förundersökning~~	
⋮ ⋮ ⋮	
~~elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.~~	

SKÄL: Tvångsmedel tillämpas inom en förundersökning, inte utanför en förundersökning. De brottsbekämpande myndigheterna kan inte sitta och hackzor-fiska på internätet efter människor att misstänka, utan behöver lägga band på tangentbordsfingrarna när de inte faktiskt har något att gå på.
Relevanta delar av 8 § har införlivats i Dataskydd.net:s förslag till ändringar i 4 § ovan.

ÄNDRING 4

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 13 §	Lag om hemlig dataavläsning, 13 §
Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. ~~En ansökan om en åtgärd i fall som anges i 8 § ska dock göras av Säkerhetspolisen eller Polismyndigheten.~~ I ett tillstånd till hemlig dataavläsning ska det anges 1. vilken tid tillståndet avser, 2. vilket informationssystem tillståndet avser, 3. vilken typ av uppgift enligt 2 § första stycket tillståndet avser, 4. i förekommande fall, den plats tillståndet gäller, och 5. vid åtgärd enligt 2 § första stycket 5 vem som är skäligen misstänkt för brottet. Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet. När tillståndet ska förenas med särskilt tillstånd enligt 12 §, ska det anges särskilt i beslutet. I tillståndet ska också i övrigt anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.	Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. I ett tillstånd till hemlig dataavläsning ska det anges 1. vilken tid tillståndet avser, 2. vilket informationssystem tillståndet avser, 3. vilken typ av uppgift enligt 2 § första stycket tillståndet avser, 4. i förekommande fall, den plats tillståndet gäller, och 5. vid åtgärd enligt 2 § första stycket 5 vem som är skäligen misstänkt för brottet. Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet. När tillståndet ska förenas med särskilt tillstånd enligt 12 §, ska det anges särskilt i beslutet. I tillståndet ska också i övrigt anges villkor för att tillgodose intresset av att enskildas personliga integritet samt *enskildas och samhällets intresse av informationssäkerhet* inte kränks i onödan*, samt i vilken utsträckning aktsamhet i enlighet med 20 § och 31 § i denna lag ska utövas, särskilt med avseende på återställande av informationssystem till deras ursprungliga säkerhetsnivå.*

SKÄL: I vår skrivelse till utredningen påtalade vi att Rättsmedicinalverket var onödigt nervösa över hur osäkert deras förfarande att lämna ut uppgifter var. Rättsmedicinalverket hade då framfört till Justitiedepartementet att de trodde att deras utlämningar av uppgifter var så tekniskt osäkra att de bara genom en egen registerförfattning kunde få förtroende hos de som tog emot uppgifterna. Ett bra sätt att få förtroende är emellertid genom att genomföra lämpliga tekniska och organisatoriska åtgärder för ett säkert utlämnande. Dataskydd.net gav förslag på olika lösningar för säkra utlämnanden av uppgifter. Vissa myndigheter har säkra utlämnanden av uppgifter, till exempel Domstolsverket och Myndigheten för samhällsskydd- och beredskap. Genom att tydligare påtala hur Rättsmedicinalverket genom att uppfylla sina skyldigheter enligt brottsdatalag kan bli trovärdigare, kan lagen hjälpa Rättsmedicinalverket att överkomma problemet med osäkra utlämningar.

Ändring 5

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 14 §	Lag om hemlig dataavläsning, 14 § (tas bort)
~~Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller möjligheterna att förhindra den brottsliga verksamheten att inhämta rättens tillstånd till hemlig dataavläsning, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut. Sådant tillstånd får dock inte avse hemlig dataavläsning enligt 2 § första stycket 5 eller hemlig dataavläsning i fall som anges i 8 §.~~ ~~Om åklagaren har gett ett sådant tillstånd, ska han eller hon utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.~~ ~~Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.~~	

SKÄL: Under ett utvärderingsstadium bör man, för denna typ av extrema åtgärd, hålla sig inom ramen för föregående, oberoende prövningar i domstol så som krävs av Europakonventionen, Sveriges grundlag och andra rättighetsdokument. Skulle det visa sig att det uppstår en massa situationer där polisen snabbt behöver hacka någon utan domstols föregående, konstitutionsenliga, oberoende, rättssäkra tillstånd kan man ju alltid försämra rättssäkerheten i Sverige i ett senare skede. Dataskydd.net anser det i allmänhet beklagligt att regeringen förefaller förutsätta att den föregående, oberoende granskning som avkrävs Sverige enligt Sveriges internationella åtaganden inte skulle vara en fullt fungerande rättssäkerhetsmekanism.

Ändring 6

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 23 § 1 st	Lag om hemlig dataavläsning, 23 § 1 st (tas bort)
~~När hemlig dataavläsning används eller har använts under förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden.~~ ~~När hemlig dataavläsning används eller har använts enligt 2 § första stycket 5 ska dock i stället det som enligt de bestämmelserna gäller för hemlig rumsavlyssning tillämpas.~~	

SKÄL: Under ett utvärderingsstadium bör Sverige tillnärma sig de internationellt sett mer normala reglerna att brottsbekämpande myndigheter inte får använda hemliga tvångsmedel för att genomföra fiskeexpeditioner i misstänkas privata kommunikationer. Behandlingen av överskottsinformation i utredningen är över lag mycket dålig, och tar inte i beaktande den ofta extremt privata natur som uppgifter har som lagras i telefoner, datorer, på sociala media-konton och i dylika utrymmen.

ÄNDRING 7

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 24 §	Lag om hemlig dataavläsning, 24 § (tas bort)
~~När hemlig dataavläsning används eller har använts i fall som anges i 6 § ska det som gäller enligt 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas för åtgärden.~~ ~~För underrättelse till enskild vid hemlig dataavläsning i fall som anges i 6 § gäller det som anges i 16–18 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som där anges om hemlig avlyssning av elektronisk kommunikation ska alltid tillämpas för hemlig dataavläsning. Det som anges om hemlig kameraövervakning ska tillämpas för hemlig dataavläsning enligt 2 § första stycket 4.~~	

SKÄL: Ändringen följer av förslaget att ta bort 6 § enligt ovan. Normalt ska ett helt nytt, mycket allvarligt och inkräktande, tvångsmedel inte omedelbart ges det vidast möjliga tillämpningsområdet. Om polisen uppger att de vill utreda barnpornografibrott och terroristbrott – låt dem göra det inom ramen för sådana utredningar där de har en misstänkt, där det faktiskt skett ett brott, och under ordnade former som i alla fall rimligt mycket liknar omständigheter i andra länder.

ÄNDRING 8

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 25 §	Lag om hemlig dataavläsning, 25 §
Vid tillämpning av 23 *och 24 §§* ska begreppet informationssystem användas i stället för telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning när något av dessa begrepp används i de hänvisade bestämmelserna.	Vid tillämpning av 23 § ska begreppet informationssystem användas i stället för telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning när något av dessa begrepp används i de hänvisade bestämmelserna.

SKÄL: Ändringen följer av förslaget at ta bort 6 §, följdrevisionen i 24 § och ändringarna i 23 § med avseende på överskottsinformation.

ÄNDRING 9

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 26–27 §§	Lag om hemlig dataavläsning, 26–27 §§ (tas bort)
~~När hemlig dataavläsning~~… …~~ underrättelseverksamhet tillämpas för åtgärden.~~	

SKÄL: Ändringen följer av förslaget att ta bort 6-10 §§.

ÄNDRING 10

Utredarens förslag	Dataskydd.net:s förslag
Lag om hemlig dataavläsning, 28 §	Lag om hemlig dataavläsning, 28 §
Frågor om tillstånd till hemlig dataavläsning prövas, om förundersökning pågår, av domstol som föreskrivs i 19 kap. rättegångsbalken. ~~Vid förundersökning om brott som anges i 27 kap. 2 § andra stycket 2–8 rättegångsbalken får sådana frågor också prövas av Stockholms tingsrätt.~~ ~~Frågor om tillstånd till hemlig dataavläsning i fall som anges i 6–10 §§ prövas av Stockholms tingsrätt.~~	Frågor om tillstånd till hemlig dataavläsning prövas, om förundersökning pågår, av domstol som föreskrivs i 19 kap. rättegångsbalken.

SKÄL: Ändringen följer av förslagen att ändra 4 §, och ta bort 6-10 §§.

Fast i gamla hjulspår om åklagarhast och överskottsinformation

Dataskydd.net ser det som positivt att utredaren inte anser att överskottsinformation ska få användas som faller utanför det tillämpliga tillståndet. Men vi anser att förslaget bör gå längre. Utredaren har uppenbarligen kört fast i gamla hjulspår vad avser överskottsinformation för den uppgiftstyp tillståndet avser.[2] Vi menar i stället att man tills att ett behov är demonstrerat av att använda överskottsuppgifter, något sådant behov inte behöver tillfredsställas. Eller alternativt: lös problem som finns, inte problem som inte finns.

Vi kan inte vara eniga med att ”[d]e rättssäkerhetsgarantier som uppställs i gällande regler om hem- liga tvångsmedel vid interimistisk åklagarprövning är tillräckliga även för att tillåta sådana beslut beträffande hemlig dataavläsning.”[3] Här verkar utredaren bara hänvisa till tradition, men tradition kan också vara dålig (exempelvis traditionen att prostituera sig, traditionen att supa sig redlös på helger, eller traditionerna att slå kvinnor eller aga barn). I fallet med interimistiska prövningar är traditionen ingen tillförlitlig vindflöjel, utan dessa bör komma på tal först i framtida lagändringar om det visar sig att det tillräckligt ofta uppstår ett behov av att snabbt hacka någon. I typfallet kan man inte anta att det är särskilt tidskritiskt att hacka någon. Bara den tekniska komplexiteten i åtgärden skapar redan ett sådant behov av förberedelser att myndigheterna med enkelhet kan invänta domstols föregående, obereoende prövning på det sätt som ju mänskliga rättighetskonventioner egentligen kräver.

Venedigkommissionens checklista för rättssäkerhet och rättsstater rör många av frågeställningarna just uppdelningen av uppdrag mellan olika myndigheter.[4]

[2] SOU 2017:89, s. 414–415.

[3] SOU 2017:89, s. 388.

[4] *Rule of Law Checklist* (CDL-AD(2016)007), Study No. 711 / 2013, Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016), Endorsed by the Ministers' Deputies at the 1263th Meeting (6-7 September 2016), Endorsed by the Congress of Local and Regional Authorities of the Council of Europe at its 31st Session (19-21 October 2016).

Men i Sverige finns, till skillnad från i Storbritannien och USA, inga starka väggar mellan myndigheterna. Vi har fri bevisprövning i våra domstolar, vilket innebär att en domstol inte nödvändigtvis kommer att undersöka metoden genom vilken en viss bevisning förvärvats var laglig. I exempelvis USA, men också i Belgien, måste bevisning ha framställts på ett lagligt sätt för att få tas i beaktande av domstol. Det skapar ett starkt incitament för brottsbekämpande myndigheter att följa lagen, som helt saknas i Sverige.

Sverige saknar en konstitution. Medborgare har inget omedelbart sätt att kräva överprövning av lagar som styr olika myndighetsfunktioner, särskilt på underrättelseområdet. Dessa möjligheter finns i de flesta andra länder, vilket skapar starkare rättssäkerhet.

Därtill är det inte uppenbart att förutsebarhetskrav tolkas på samma sätt i den svenska myndighetsapparaten som i de internationella organ som tillser mänskliga rättigheter världen över och i Europa, och medan en stor medvetenhet byggts upp i den internationella människorättsdoktrinen kring potentiella integritetskränkningar som följer av profilering, beteendekartläggning och andra former av metadatabehandling är Sverige fortfarande kvar i samma tankebanor som på 1980-talet (Integritetskommittén undantagen). Faktum är att det skett en tillbakagång i Sverige, eftersom man på 1970-talet var ytterst medveten om exempelvis samkörningsproblem men idag sopar dem under mattan. Sverige saknar också en utvecklad debatt – särskilt inom ramen för statliga utredningar – om automatiskt beslutsfattande och kontrollåtgärder.

Eftersom en brottsutredning kan framställa bevisning som tillkommit olovligt — till exempel genom skvaller mellan myndigheter som är ålagda begränsningar och underställda tillsyn och myndigheter som är ålagda få begränsningar på sina verksamheter och som bara svårligen kan underställas tillsyn — utan att ifrågasättas av domstolen, kan man anta att så kommer ske. Inte heller kan någon utanför rättsväsendet på något enkelt eller lagligt sätt påvisa att överträdelser har skett, och då finns en risk för missbruk.[5] Både regeringskansliet, statliga utredare och de brottsbekämpande myndigheter behöver vara medvetna om att *när de tar intryck av brottsbekämpningsmetoder som används i andra rättsliga system än det svenska, så är de brottsbekämpningsmetoderna i de rättsliga systemen underställa rättssäkerhetsgarantier som inte finns i Sverige*. Inverkan av vidlyftiga regler om överskottsinformation och åklagarprövning och hacking blir alltså *värre* i Sverige, för att Sverige traditionellt saknat starka domstolar, har fri bevisprövning, och saknat avgränsade, specifika tvångsmedelsförfrågningar eller starka väggar mellan brottsbekämpande myndigheter, säkerhetsmyndigheter, och så vidare.

Missbruksrisk uppstår sedan på grund av det som kallas *incitamentslära* eller *rational choice*. Om det är rationellt, effektivt och enkelt för en aktör att bete sig på ett visst sätt som uppfattas som gynnsamt för den aktören, kommer aktören sannolikt att bete sig på det sättet. När åklagare och andra brottsbekämpande

[5] Dataskydd.net har tagit upp detta även i vårt remissyttrande över SOU 2016:7 om stärkt straffskydd för integriteten.

myndigheter[6] får möjlighet att bete sig dåligt för att göra arbetet lite enklare, kommer de bete sig dåligt för att göra arbetet lite enklare *eftersom det vore dumt att låta bli*.

Incitamentsläran innebär inte att dessa myndigheter är ondskefulla bara för att de gör det som är lättast. Det är inte heller givet att någon av myndigheterna alltid kommer att agera på det sätt som är mest rationellt i bemärkelsen att det kräver minst arbete. Däremot vore det bara dumt av myndigheterna att aldrig agera rationellt i denna bemärkelse. De svenska informationsdelningsstrukturerna lånar sig helt enkelt väl till missbruk, och då är det rimligt att anta att missbruk kommer ske.

Åtgärder som försämrar informationssäkerhet för enskilda och konsumenter

I inlagorna till utredningarna om modernisering av beslag och husrannsakan (Ju 2016:08)[7], hemlig dataavläsning (Ju 2016:12)[8] och utredningen om personuppgiftsbehandling inom Försvarets radioanstalt[9] har Dataskydd.net utvecklat hur användningen av *sanktionerade dataintrång* (det som i den försvarsorienterade verksamheten kallas för *offensiv IT-säkerhet*) skadar konsumenters och privatpersoners intressen av pålitliga, tekniska verktyg att genomföra sina dagliga kommersiella och sociala sysslor, samt uppfylla sina förpliktelser gentemot offentliga organ.

Vi gör följande terminologiska uppdelningar:

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.	Teknisk 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.	Juridisk säkerhet.
Sanktionerade dataintrång	Att hacka, begå dataintrång, genomföra hemlig dataavläsning, husrannsakan i en dator, husrannsakan på distans och offensiv IT-säkerhet	Sanktionerade dataintrång.

[6] Och Dataskydd.net vill här understryka att åklagare faktiskt är en del av den brottsbekämpande apparaten, trots att exempel SOU 2017:75 om datalagring och integritet på något sätt lyckades få åklagare till *oberoende* av brottsbekämpning(?!). Se vårt remissyttrande över SOU 2017:75, Datalagring och integritet.

[7] Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI), skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan.

[8] Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI), skrivelse till utredningen om hemlig dataavläsning.

[9] Dataskydd.net, skrivelse till utredningen om dataskydd inom Försvarsmakten och på Försvarets radioanstalt (dir. 2017:42).

	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, kopiera, radera eller manipulera data, filer, eller programvaror) på utrustningen. Vi kommer att använda begreppet ”sanktionerade dataintrång” som samlingsterm för samtliga dessa begrepp.	
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).	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 kan också innebära till exempel att man gör en ny och bättre standard för den bakomliggande utrustningen.	Åtgärda en sårbarhet.
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 *o-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.	o-day.
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 *o-day*).	Metoder för att utnyttja sårbarheter.

En offensiv IT-säkerhetsåtgärd gör inte bara skada vid själva avlyssnings- och övervakningstillfället, utan kan fortsätta göra skada tills dess att de tekniska åtgärder som vidtagits av underrättelsemyndigheterna 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.

Den kan också 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,[10] och för de oavsiktligen drabbade finns ingen hjälp att få så länge det inte är känt hur man kan laga det introducerade säkerhetsproblemet. Senast under våren 2017 drabbades flertalet större administrativa system för offentliga verksamheter inom kommuner och i sjukvården, i både Sverige[11] och utomlands,[12] av utpressningstrojanen WannaCry. Trojanen utvecklades i sin tur på bas av underrättelseutvecklade metoder för att utnyttja sårbarheter i ett IT-system.[13]

Sanktionerade dataintrång, oavsett vad man kallar dem, har alltså redan bevisligen orsakat risker och skador för civila verksamheter i hela världen, till en hög kostnad, och det finns inga sätt att garantera att just de sanktionerade dataintrång som svenska försvarsmyndigheter och underrättelsemyndigheter eller säkerhetstjänster ägnar sig åt i den offensiva IT-säkerhetens namn inte kommer att orsaka motsvarande skador. Förfarandet bör alltså av säkerhetsskäl och hänsyn till de icke-militära verksamheterna begränsas.

Egalt vems fel attackmjukvaran är. För att sjukhus är det ovidkommande vem som utvecklat en attackmjukvara eller sårbarheterna och metoderna att utnyttja sårbarheterna som attackmjukvaran använder sig av. Om flertalet datorer låser sig till följd av en utpressningstrojan så är det ju så, även om sårbarheten som trojanen använder för att snirkla sig in i datorn utvecklades av en (svensk) underrättelsetjänst.

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.[14,15,16,17] 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,[18] men den är ofta också inte vit och inte kartlagd.[19] 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.[20] Behovet av regler för denna marknad har lyfts i europeiska sammanhang av bland andra europeiska dataskyddstillsynsmannen,[21] men i Sverige saknas en sådan diskussion.

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

[11] NyTeknik. Kalle Wiklund (17 maj 2017) Timrå kommun: Miss hos it-leverantör öppnade för Wannacry.

[12] The Guardian. Alex Hern och Samuel Gibbs (12 maj 2017) What is WannaCry ransomware and why is it attacking global computers?

[13] Wired. Matt Burgess (28 juni 2017) Everything you need to know about EternalBlue – the NSA exploit linked to Petya.

[14] Andy Greenberg (21 March 2012). ”Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)” Forbes.

[15] Adrianne Jeffries (13 September 2013). ”Meet Hacking Team, the company that helps the police hack you” The Verge.

[16] Vernon Silver (8 november 2012) ”MJM as Personified Evil Says Spyware Saves Lives Not Kills Them” Bloomberg.

[17] Der Spiegel, 9 november 2014 ”BND will Informationen ueber Software-Sicherheitsluecken einkaufen”.

[18] Se ovan fotnot 14.

[19] SpiderLabs Research (31 maj 2016) Zero Day Auction for the Masses, Trustwave Spiderlabs Blog.

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

[21] 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)[22] 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 underrättelsemyndigheter, blir dessa företag en egen intressegrupp som utövar politiskt inflytande på de underrättelsemyndigheterna 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.[23,24,25] Företagens egenintresse kan antas vara att framställa sig som ovärderliga och nödvändiga för effektiv underrättelseverksamhet, eftersom deras huvudsakliga intäktskälla är just samarbete med underrättelsemyndigheter.

Det här skapar ett behov av ytterligare regler kring hur brottsbekämpande myndigheter får befatta sig med sårbarheter, så att inte de brottsbekämpande myndigheterna börjar agera menligt mot den egna befolkningens intressen av säkerhet i IT-system. Vi har alla ett intresse av att våra smartphones, våra webbläsare och våra arbetsstationer fungerar på det sätt vi tror och vill att de ska göra.

Missförstånd om säkerhetsekonomi i utredningen

Utredaren har invänt mot två av Dataskydd.net:s och DFRI:s huvudsakliga poänger, som anknöt till att säkerhet är i lika delar en ekonomisk fråga som det är en teknisk. Det är dyrt och svårt att upprätthålla god säkerhet, och det blir mycket dyrare och svårare att upprätthålla god säkerhet om de brottsbekämpande myndigheterna får operativa incitament att försämra säkerheten.

Utredaren menar att domstolar inte kan bedöma hur en tvångsåtgärd ska genomföras.[26] Men hur tvångsåtgärden genomförs är avgörande för om aktsamhetskravet utredaren föreslår i 20 § kan efterlevas! Antingen menar utredaren att aktsamhetskravet i 20 § är fina ord utan praktisk betydelse, eller så har utredaren inte förstått hur ett aktsamhetskrav faktiskt praktiskt måste genomföras. Därför föreslår vi att aktsamhetskravet ska ingå i det som ska redovisas för domstolen. Dataskydd.net noterar även att det på alla andra sätt saknas möjligheter både för den drabbade och för allmänheten att informera sig om de brottsbekämpande myndigheternas säkerhetssänkande aktiviteter.

Utredaren menar också att det saknas behov av att beskriva vilka sårbarheter och metoder för utnyttjande av sårbarheter som använts för att orsaka en viss sorts informationssäkerhetsproblem (som ju alla sanktionerade dataintrång

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

[23] 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.

[24] 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.

[25] 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.

[26] SOU 2017:89, s. 396.

egentligen är).[27] Men dessa sårbarheter och metoder bör redovisas för att det ska vara så enkelt som möjligt att återställa system till sin ursprungliga säkerhetsnivå. Så att myndigheternas åtgärder inte orsakar mer skada än vad de löser, helt enkelt. Dataskydd.net och DFRI detaljerade i sin skrivelse till utredningen varför det är så att insyn och transparens i sårbarheter och metoder för att utnyttja dessa skapar förutsättningar för systeminnehavare att laga sina informationssystem. Genom att ålägga de brottsbekämpande myndigheterna med ytterligare transparenskrav kanske till och med säkerheten kan förbättras och återställas i samma takt som de brottsbekämpande myndigheterna förstör den.

Vi tror att redovisningar av de tilltänkta metoderna för aktsamhet enligt 20 § redan vid tillståndsprövningen kan vara tillräckligt för att åtgärda båda problemen, eventuellt i kombination med en viss alerthet hos domstolarna. Att domstolar i dagsläget saknar förmåga och kompetens att bedöma tekniska och ekonomiska implikationer av de brottsbekämpande myndigheterna åverkan på samhällets informationssäkerhet, anser vi inte vara något gott skäl att anta att domstoler kommer fortsätta vara inkompetenta på detta område. Tvärtom har vi stort förtroende för att domstolarna kommer lyfta sig, skaffa kunskaper och säkerställa att allmänheten och det allmänna inte drabbas negativt av polishacking.

Amelia Andersdotter
Ordförande, Dataskydd.net

[27] Ibid., s. 397–398.