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: Det kongelige forsvarsdepartementet, Norge

Svar till Høring - Forslag til ny lov om Etterretningstjenesten

Er ref.: 2016/2773-5/FD II 4/SIH

12 februari 2019

Föreningen för digitala fri- och rättigheter (DFRI) är en svensk 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 svensk 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]

Vi vill börja med att välkomna att det kungliga försvarsdepartementet lagt stor vikt vid människorättens växande betydelse i norsk lagstiftning under senare år. Frågorna som hanteras i förslaget medför svåra avvägningar i detta avseende och fokuset på tillsynsmekanismer, särskilt att tillsynsmekanismerna föreslås ligga inom det vanliga rättsväsendet[3] snarare än upprättas som särskild och avskild instans, är mycket önskvärt.

Detta yttrande är skrivet så, att det börjar med en hänvisning till internationell praxis, för att sedan gå in på specifika invändningar mot delar av försvarsdepartementets förslag.

De sorters förfaranden som försvarsdepartementet menar är nödvändiga har tidigare kritiserats av bland annat Europarådets parlamentariska utskott PACE,[4] upprepade gånger av flertalet organ i Förenta nationerna[5] och av Europarådets

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

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

[3] Høringsnotat, Forslag til ny lov om Etterretningstjenesten, s. 18.

[4] 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).

[5] *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, A.HRC.23.40 EN av 17 april 2013; FN:s kammare för mänskliga rättigheter, 27 sessionen, A/HRC/27/37 av den 30 juni 2014; FN:s generalförsamling, 69 sessionen, A/69/397 av 23 september 2014; General Assembly resolution A/C.3/69/L.26/Rev.1, *The right to privacy in the digital age*, av 25 november 2014; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the General Assembly*, A/70/361, av 8 september 2015.

människorättskommissionär.[6] Förfarandena som norska försvarsdepartementet menar att norsk underrättelsetjänst behöver få utföra mot personer i och utanför Norge är därtill under prövning i Europadomstolens stora kammare[7] och i ytterligare mål i Europadomstolens underkammare.[8] Generell övervakning som inte riktas mot någon särskild, sedan tidigare misstänkt, person, och som därigenom drabbar alla privatpersoner, utan åtskillnad, har prövats även i Europeiska unionens domstol[9] och kommer genom en hänskjuten från belgiska högsta domstolen att prövas i EUD även utifrån det nationella säkerhetsperspektivet.[10]

Mot bakgrund av den starka kritik som det internationella samfundet riktat mot den sortens metoder som försvarsdepartementet föreslår ska införlivas i norsk underrättelseverksamhet, vill vi därför uppmuntra norska lagstiftare att fortskrida försiktigt. I vissa delar menar vi att den norska lagstiftaren helt bör undvika att gå på försvarsdepartementets linje:

Avstyrkes: bulkaksess och tilrettelagt innhenting (§7-2, §7-4)

Vi invänder skarpt mot förslagen att genom §7-2 och §7-4 i den nya lagen tvinga norska telekommunikationsbolag att delta i urskiljningslös övervakning av all elektronisk trafik som färdas över gränsen mellan Norge och Sverige.

Vi ser detta som en kränkning av både norska och svenska medborgares mänskliga rättigheter, som vår rätt till personlighet, åsiktsfrihet och privatliv. Att "*spørsmålet om søk i slik kommunikasjon behandles særskilt både i høringsnotatet og i lovutkastet, og at de tilhørende kontrolltiltakene som foreslås er meget strenge*"[11] hjälper inte, eftersom kränkningen av våra mänskliga rättigheter uppstår vid övervakningstillfället, och inte i den administrativa hanteringen av övervakningen. En stat kan inte lägga över på en maskin att genomföra en människorättskränkande åtgärd, och sedan förvänta sig att denna kränkning inte har effekter för de som blir utsatta för kränkningen.

Forskning visar att massövervakning påverkar människors beteende på ett negativt sätt.[12] Den obehagliga känslan av att ständigt vara observerad leder till oro och ökad otrygghet.[13] Staten bör inte vidta åtgärder som riskerar att någon tvekar att söka hjälp genom att kontakta exempelvis en psykiatrisk mottagning, av rädsla för att det registreras och sparas. Alla ska kunna läsa om känsliga ämnen på ungdomsmottagningens webbsida utan att vara orolig för att det övervakas, och medborgare i ett fritt samhälle ska inte behöva oroa sig för hur deras samtalslistor eller deras surfhistorik kan tolkas eller missförstås. Under massö-

[6] CommDH/IssuePaper(2014)1, *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights*, 8 december 2014.

[7] ECHR 053 (2019), *Big Brother Watch and Others v. the United Kingdom* (application nos. 58170/13, 62322/14 and 24960/15), 5 februari 2019.

[8] Privacy International, Privacy International and Others v. United Kingdom (UK Government Hacking), European Court of Human Rights, Application No. 46259/16.

[9] ECLI:EU:C:2017:222, C-203/15. Tele2 och ECLI:EU:C:2017:222, C-698/15. Watson, men se även ECLI:EU:C:2014:238, C-293/12. Digital Rights Ireland.

[10] Europeiska unionens domstol, EUT C 408, 12.11.2018, s.39 (mål C-520/18).

[11] Se s. 192 i fotnot 3.

[12] J. W. Penney, *Internet surveillance, regulation, and chilling effects online: a comparative case study*, Internet Policy Review Vol. 6; J. W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Technology Law Journal Vol. 31. För en sammanfattning, se även Jonathan Shaw, *The Watchers*, Harvard Magazine, jan-feb 2017.

[13] Se ex. Internetstiftelsen i samarbete med Insight Intelligence och SICS samt svenska näringslivsaktörer och Stockholms landsting, Delade meningar 2, mars 2016. Andra opinionsmätningar finns, exempelvis 2016 CIGI-Ipsos Global Survey on Internet Security and Trust.

vervakning är det inte självklart att man fritt vågar utnyttja yttrandefriheten,[14] speciellt om man har en avvikande eller mindre populär åsikt.[15] Övervakningen riskerar därför att skada det demokratiska samhället snarare än att skydda det.[16]

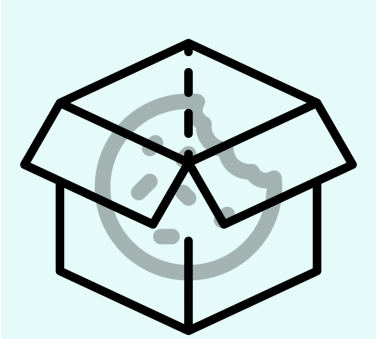
Norge har länge varit en global förebild för demokrati[17] och en demokratisk metodik för rättsväsendet.[18] Vi hoppas att Norge kommer fortsätta vara en symbol för demokrati och mänskliga rättigheter, i en värld där allt fler stater hängivit sig åt nationalism, isolationalism och egenintresse.[19] Mot bakgrund av de tre pågående domstolsprövningar av denna sorts förfaranden hänvisade till ovan,[20] menar vi att Norge fortsatt bör avvakta i stället för att lagstifta.

Avstyrkes: ilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering (§7-2.d)

Vi är starkt kritiska mot förslaget i §7-2 att norska underrättelsetjänsten ska ges befogenheter att sabotera webbkryptering och annan kryptering som används i vanliga konsumentprodukter. Att departementet ”*ikke på noen måte vil svekke sikkerheten som kryptering gir*”[21] hjälper inte. Man kan inte både attackera en säkerhetsmetod och/eller förbjuda näringsidkare att tillämpa denna säkerhetsmetod i syfte att omintetgöra den och samtidigt bevara den.

Kryptering är det bästa och i många fall enda sättet privatpersoner i både Sverige och Norge har idag för att skydda sina konsumenträttigheter och sina rättigheter som individer. Det gäller för journalister, aktivister och oppositionella, verksamma i länder med mindre människorättsvänliga ambitioner än Norge, som behöver skydda sin verksamhet.[22]

Genom att uttryckligen uppdra åt underrättelsetjänsten eller åt andra myndigheter att försvaga och försämra, motarbeta och förbjuda eller utveckla attacker mot, dessa skyddsåtgärder blir människor inte bara i Norge, utan över hela världen, försatta i sämre ställning att skydda sina rättigheter. Denna sämre



Schrödingers kaka. Schrödingers katt är ett tankeexperiment skapat av den österrikiske fysikern Erwin Schrödinger för att illustrera den stokastiska naturen i modellerna vi använder för att beskriva våg-partikel-dualitet hos elementärpartiklar. Dessa modeller har ingen egentlig bäring på den makroskopiska tillvaro vi befinner oss i.

Ikoner av Ralf Schmitzer (DE) och Tinashe Mugayi (MY) via NounProject CC BY.

[14] PEN America, Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor, 12 november 2013.

[15] Julius Endnert (DW), *Digital security crucial to protecting human rights*, 25 januari 2017.

> *Online surveillance is exploding, and people are increasingly facing threats or being detained because of their online activities." This gloomy assessment made by DW Akademie in 2016 is even more of a reality today. /.../ [The Committee to Protect Journalists], for example, says that online is now one of the ten most dangerous places for journalists to work, on par with countries like Egypt or Syria.*
>
> *This is partly because authoritarian governments, intelligence agencies and criminal organizations are now able to use the Internet more 'professionally' than ever before. Not only do they have a huge digital arsenal at their disposal, ranging from surveillance software (spyware) to social network data, but their targets (e.g., journalists, human rights defenders) often know little about digital security, leaving them vulnerable to attack.*

[16] Det finns relativt omfattande litteratur på området. Vi rekommenderar särskilt J. Fairfield och C. Engel, *Privacy as a public good*, Duke Law Journal Vol. 65, december 2015, och T. Stahl, *Indiscriminate mass surveillance and the public sphere*, Ethics and Information Technology Vol. 18, mars 2016.

[17] Jfr. Fredspriset till Nobels minne.

[18] Jfr. hanteringen av högerextremistiska våldsverkare efter Utøya-massakern.

[19] Dessa tre begrepp ska här förstås som att den lokala staten ber medborgarna att "räkna till tio och tänk på kungen" snarare än räkna med den lokala staten som bärare av medborgarnas rättigheter.

[20] Se ovan, fotnot 7, fotnot 8 och fotnot 10.

[21] Se ovan, fotnot 3.

[22] Se bl. a. Morgan Marquis-Boire et al. i ett antal Citizen Labs Toronto-rapporter men även ovan fotnot 12, 14 eller 15.

ställning uppstår inte nödvändigtvis gentemot norska staten.[23] Den sämre ställningen uppstår i stället gentemot privata tjänsteleverantörer, gentemot andra stater och i mellanmänskliga relationer.

I ett inspel i ett svenskt förfarande framförde våra organisationer gemensamt följande uppdelning:[24]

> ”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” 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. /.../
>
> [I elektroniska miljöer är den juridiska säkerheten för konsumenter svag, bland annat genom flyttad bevisbörda vid användning av elektroniska signaturer.] Detta har redan drabbat svenska konsumenter negativt i sådan utsträckning att det skrivits om det i media under flera år. Att den juridiska risken ligger på konsumenten ökar behovet av [teknisk] säkerhet i konsumentens egna verktyg (webbläsare, e-postklient, operativsystem, osv.), så att lösenord, inloggningsuppgifter, kredituppgifter och dylikt inte kan avhändas konsumenten via någon sorts dataintrång. /.../
>
> 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.

Det är svårt att tillräckligt understryka dessa nästan helt igenom konsumenträttsliga effekterna av försvarsdepartementets förslag. En analys av inverkan av försvarsdepartementets förslag på helt vanliga vardagssituationer som nästan varje norrman och svensk anträffar varje dag saknas helt i kartläggningen av hotbilden.[25] Stuprörstänket som ofta återfinns i politiken, där konsumenter ägnar sig åt konsumentfrågor, och militärer ägnar sig åt säkerhetsfrågor, riskerar att innebära långsiktiga skador för privatpersoner i Norges och Sveriges säkerhet. Förslagen som försvarsdepartementet lagt fram är olyckligtvis ytterligare ett exempel på det bland många.

---

[23] Det är nämligen i alla fall teoretiskt möjligt att administrativt kontrollera en stats interna handlingar, så som försvarsdepartementet föreslår att Oslo tingsrätt ska göra.

[24] DFRI:s och Dataskydd.net:s gemensamma inspel till den svenska utredningen om hemlig dataavläsning.

[25] Se s. 93 i fotnot 3.

Referenser

Huvudsakliga

1. Conseil d'État (Högsta förvaltningsdomstolen, Frankrike), Le numérique et les droits fondamentaux, 2014. http://www.ladocumentationfrancaise.fr/rapports-publics/144000541/index.shtml
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. Europeiska unionens domstol, ECLI:EU:C:2014:238, C-293/12. Digital Rights Ireland. http://curia.europa.eu/juris/documents.jsf?num=C-293/12
4. Europeiska unionens domstol, ECLI:EU:C:2017:222, C-203/15. Tele2. http://curia.europa.eu/juris/documents.jsf?num=C-203/15
5. Europeiska unionens domstol, ECLI:EU:C:2017:222, C-698/15. Watson. http://curia.europa.eu/juris/documents.jsf?num=C-698/15
6. Europeiska unionens domstol, EUT C 408, 12.11.2018, s.39 (mål C-520/18). http://curia.europa.eu/juris/fiche.jsf?id=C%3B520%3B18%3BRP%3B1%3BP%3B1%3BC2018%2F0520%2FP
7. ECHR 053 (2019), 5 februari 2019, *Big Brother Watch and Others v. the United Kingdom* (application nos. 58170/13, 62322/14 and 24960/15). http://hudoc.echr.coe.int/eng-press?i=003-6321717-8260093
8. Europarådet, CommDH/IssuePaper(2014)1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights*. https://wcd.coe.int/ViewDoc.jsp?id=2268589&Site=COE
9. F. Verbruggen, S. Royer och H. Severijns, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, 1 oktober 2018. http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/
10. Förenta nationerna, Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression. Rapport A.HRC.23.40 EN av 17 april 2013. http://ap.ohchr.org/documents/dpage_e.aspx?m=85
11. Förenta nationerna, FN:s kammare för mänskliga rättigheter, 27 sessionen. Rapport A.HRC.27.37 av den 30 juni 2014. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=23880
12. Förenta nationerna, Rapporter om mänskliga rättigheter till FN:s generalförsamling, 69 sessionen. Rapport A.69.397 av 23 september 2014. http://www.ohchr.org/EN/newyork/Pages/HRreportstothe69thsessionGA.aspx
13. Förenta nationerna, General Assembly resolution A/C.3/69/L.26/Rev.1, The right to privacy in the digital age, av 25 november 2014. http://www.un.org/en/ga/third/69/propslist.shtml
14. Förenta nationerna, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the General Assembly. Rapport A/70/361, av 8 september 2015. http://ap.ohchr.org/documents/dpage_e.aspx?m=85
15. J. W. Penney, *Internet surveillance, regulation, and chilling effects online: a comparative case study*, Internet Policy Review Vol. 6. https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case
16. J. W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Technology Law Journal Vol. 31. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://scholar.google.se/&httpsredir=1&article=2104&context=btljz
17. PEN America, Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor, 12 november 2013. https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf

18. Privacy International, Privacy International and Others v. United Kingdom (UK Government Hacking), European Court of Human Rights, Application No. 46259/16. https://privacyinternational.org/legal-action/privacy-international-and-others-v-united-kingdom-uk-government-hacking

Övriga

19. DFRI och Dataskydd.net, skrivelse till den svenska utredningen om hemlig dataavläsning, 30 juni 2016. https://dataskydd.net/sites/default/files/dir201636_dfri_dataskyddnet_slutgiltig_2.pdf

20. 2016 CIGI-Ipsos Global Survey on Internet Security and Trust https://www.cigionline.org/internet-survey-2016

21. J. Fairfield och C. Engel, *Privacy as a public good*, Duke Law Journal Vol. 65, december 2015. [FINNS EJ SOM WEBBRESURS]

22. 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

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. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

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. https://citizenlab.org/wp-content/uploads/2009/10/You-Only-Click-Twice-FinFisher%E2%80%99s-Global-Proliferation.pdf

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. 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

26. T. Stahl, *Indiscriminate mass surveillance and the public sphere*, Ethics and Information Technology Vol. 18, mars 2016. https://link.springer.com/article/10.1007/s10676-016-9392-2