Stockholms universitet

2025-10-02 Dnr SU-2829-25

Juridiska fakultetskansliet

Försvarsdepartementet

Remiss av Utkast lagrådsremiss: Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning

Inledning

I utkastet till lagrådsremiss föreslås en ny signalspaningslag i krig och krigsfara, medan nuvarande signalspaningslag kommer att gälla bara i fred. Vidare föreslås bl.a. att signalspaningslagen ändras så att signalspaning fortsättningsvis också ska få omfatta ”lagrade signaler”.

Till det slutbetänkande på vilket lagrådsremissen bygger, *Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning* (SOU 2024:59), insändes ett 17 sidor långt spontant remissyttrande av professor Mark Klamberg och professor Pål Wrange (i lagrådsremissen finns det omnämnts som ett yttrande från ”två privatpersoner”). Yttrandet skrevs som ett led i verksamheten vid Stockholm Centre for International Law and Justice (SCILJ) vid Stockholms universitet. Stockholms universitet hade inte anmodats yttra sig, och de båda remissvarsförfattarna noterade, med förvåning, att remissen tillställts bara en juridisk institution i Sverige (Umeå) och att ingen juridisk institution stod på sändlistan för det tidigare betänkandet om signalspaning, “Signalspaning i försvarsunderrättelseverksamhet” (SOU 2023:51). Juridiska fakulteten uppskattar möjligheten att yttra sig över detta utkast till lagrådsremiss men noterar också att bara Umeå och Stockholms universitet beretts tillfälle att yttra sig denna gång.

Det spontana remissyttrandet, vilket bifogas, bestod av två delar. I den första delen kommenterade och kritiserade Mark Klamberg flera av utredningens förslag. Professor Klamberg har, p g a andra åtaganden, inte haft möjlighet att kommentera utkastet till lagrådsremiss. Detta innebär att juridiska fakulteten inte heller haft möjlighet att ta ställning till de frågorna. Klambergs delyttrande bör dock likafullt beaktas i den fortsatta processen på basis av styrkan av hans analys.

Stockholms universitet
106 91 Stockholm

Besöksadress:
Universitetsvägen 10 A

I remissen har Juridiska fakulteten anmodats att yttra sig om avsnitt 6.3 och 8, men fakulteten kommer bara att yttra sig över avsnitt 6.3, och i detta yttrande också till stora delar hänvisa till det tidigare yttrandet från Klamberg och Wrange.

FRA ges genom ett ”förtydligande” explicit rätt att inhämta ”lagrade signaler”

Utredningen föreslår en avsevärd förändring av FRA:s lagstadgade uppdrag och mandat genom ett tillägg av nio ord i 1 § signalspaningslagen (här kursiverade):

> I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning, *oavsett om signalerna är under förmedling eller är lagrade*. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Som ska diskuteras nedan innebär förslaget att FRA ges explicit rätt att hacka sig in i datorsystem i andra länder. Den första frågan är huruvida detta utgör en förändring av FRA:s uppdrag, och om det i så fall är en betydande förändring som förtjänar noggranna överväganden. I lagrådsremissen, liksom i utredningsbetänkandet, skrivs att detta blott utgör ett ”förtydligande” av vad som redan gäller (ss 75, 76, 79) varför det inte behövs några nya överväganden om bl.a. integritetsskydd. Som utvecklas i det tidigare remissyttrandet (ss 8-13) är det emellertid knappast förenligt med normalt språkbruk att kalla förändringen för ett förtydligande i förhållande till gällande lagstiftning. Att det utgör en kodifiering av existerande *praxis* är en annan (och i sig anmärkningsvärd) sak.

Inhämtningsförbud beträffande signaler som lagras i Sverige

Som anges i 2 a § signalspaningslagen får inhämtning inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige (s 80). Det föreslås ett förtydligande om att detta även gäller signaler som lagras i Sverige. Juridiska fakulteten har inga invändningar mot syftet med denna begränsning, dvs att skydda signaler mellan personer som befinner sig i Sverige, men är inte övertygad om att den föreslagna bestämmelsen fyller det syftet, eftersom den inte undantar signaler som lagras utanför Sverige, dvs. de allra flesta signaler. Denna fråga kommenterades i det tidigare remissyttrandet.

Rätten att vidta ”tekniska åtgärder”

I lagrådsremissen (liksom i betänkandet) föreslås att 2 § kompletteras med följande skrivning:

> Vid inhämtning enligt 1 och 1 a §§ av signaler i elektronisk form får signalspaningsmyndigheten vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtningen.

I en mening förklaras vad som menas med ”tekniska åtgärder”, nämligen att ”Försvarets radioanstalt [kan] behöva utnyttja tekniska sårbarheter, förbiseenden och inbyggda åtkomstmöjligheter i nätverksansluten utrustning” (s 80). Detta är i stort sett vad som i dagligt språk kallas hackning. Detta diskuteras i det tidigare remissvaret, där det bl.a. påpekas att utnyttjandet av sårbarheter kan medföra svåra etiska problem. Ska en säkerhetstjänst som känner till en sårbarhet i t ex Windows 11 behålla den för sig själv för att kunna utnyttja den för sina behov eller ska man underrätta tillverkaren, t ex Microsoft, så att de kan täppa till luckan? Exemplet Shadow brokers[1] visar att detta är frågor av potentiellt stor betydelse för allmänheten. De nämns dock varken i betänkandet eller i utkastet till lagrådsremiss.

Folkrättsliga aspekter

Diskussionen om ”tekniska åtgärder” leder in på de synnerligen viktiga folkrättsliga aspekterna, särskilt frågan om Sverige, inklusive FRA, har förpliktelser att respektera andra staters territorium och suveränitet. Även om det – trots vad som anförts ovan -- vore så att lagförslaget inte utgör en egentlig förändring så borde såväl utredningen som utkastet till lagrådsremiss ha tagit upp dessa frågor, eftersom det (såvitt kan utrönas) inte gjordes under lagstiftningsprocessen inför 2008 års lag. När FRAs dåvarande generaldirektör hördes av riksdagens försvarsutskott den 13 maj 2008 fick han frågan om den föreslagna lagstiftningen skulle medge aktiv signalspaning (hackning) vilket han tillbakavisade (bilaga till protokoll, utskottssammanträde 2007/08:36).

Traditionell signalspaning har utövats inom en stats gränser eller på (eller över) internationellt vatten. Den spanande staten har agerat utan att direkt kränka en annan stats suveränitet. När signalspaningen utsträcks till trådbundna signaler händer inget avgörande från ett suveränitetsperspektiv, under förutsättning att spaningen inte utförs på andra staters territorium.

Att ”signalspana” i datorsystem på andra staters territorium är en helt annan sak. Sedan 2013 är det en internationellt vedertagen uppfattning att folkrätten i stort gäller också i ”cyberrymden”, medan frågan om territoriell suveränitet i ”cyberrymden” är fortsatt kontroversiell. Ett antal stater, däribland Sverige, har avgivit positionspapper där man angett sina synpunkter på denna och andra frågor.

Den mest omdebatterade frågan internationellt är hur den territoriella suveräniteten ska förstås vad gäller olika cyberåtgärder. Frankrike, t ex, har en strikt syn och menar att ”[e]very non-authorised penetration by a state actors into French systems …may constitute, at a minimum, a violation of sovereignty”. Andra stater, som Nederländerna, har en liberalare syn medan USA och Storbritannien (men veterligen inga andra stater) anser att den territoriella suveräniteten inte gäller i ”cyberrymden” över huvud taget.[2] I Sveriges positionspapper från 2022 sägs att ”States … have an obligation to respect the

[1] En hacker-grupp med detta namn lyckades bl a komma åt amerikanska NSA:s EternalBlue-mjukvara, vilken sedan användes i två av de största hackerattackerna under senare år: NotPetya (sannolikt från Ryssland) och WannaCry (sannolikt från Nordkorea).

[2] Däremot menar man att andra regler gäller, t ex förbudet mot våldsanvändning.

sovereignty of other States."[3] Detta är allmänt uttryckt och preciserar inte om t.ex. hackning av servrar i andra stater är tillåtet, varför en hänvisning till detta papper (s 78) inte räcker som utläggning av den svenska regeringens uppfattning i denna fråga.

Förutom de rent juridiska aspekterna av dessa frågor finns det också synnerligen viktiga policyaspekter, inte minst vad gäller andra staters reaktioner på svenskt agerande eller andra staters reciproka agerande. Man måste överväga hur den regel som FRA synbarligen tillämpar, nämligen att det är tillåtet att bryta sig in datorsystem i andra länder, har för effekt för Sverige i an "whole of society"-analys. Det är uppenbart att en liberal regeltolkning har tjänat Sverige väl i så måtto att den har gett FRA möjlighet att inhämta information som är viktig för Sveriges säkerhet, men den fråga som måste ställas och diskuteras är vilka följder den kan få för andra svenska intressen. När det år 2015 avslöjades att Kina, i den s k OPM-hacken, hade skaffat sig tillgång till information om 22 miljoner federalt anställda personer i USA (en del av vilken information var synnerligen känslig), kunde den dåvarande amerikanska underrättelsechefen James Clapper inte säga annat än att han gratulerade kineserna (och skulle ha gjort likadant om han kunnat), eftersom detta agerande, enligt amerikanskt synsätt, inte bröt mot folkrätten.[4] Detta var förmodligen naturligt mot bakgrund av hur USA bedriver sin egen underrättelseverksamhet. Kan samma slutsats dras av hur FRA agerar?

I utredningsbetänkandet stod inget om dessa frågor. I utkastet till lagrådsremiss har departementet, tacknämligt nog, lagt till en halv sida om folkrättsliga aspekter (s 78). I det första stycket anges att Sverige och många andra stater inte ser något behov av några nya folkrättsliga regler på cyberområdet. Det är också Juridiska fakultetens uppfattning. Den brännande frågan är istället hur de befintliga reglerna ska tolkas, inte minst vad gäller territoriell suveränitet. Om detta sägs följande i det andra stycket:

> Underrättelseinhämtning med cybermetoder är inte underkastad ett generellt folkrättsligt förbud. Detta synsätt har bl.a. stöd i Sveriges och andra staters positionspapper om cyber och folkrätt samt i litteratur (se den av NATO Cooperative Cyber Defence Centre of Excellence upprättade webbsidan cyberlaw.ccdcoe.org och Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, andra upplagan, 2017, s. 168–174).

---

[3] Vidare:

> In general, Sweden is of the view that violations of sovereignty may arise from cyber operations that result in damage or loss of functionality. Altering and interfering with data without causing physical harm may also violate sovereignty. Such acts include those directed against cyber infrastructure belonging to private individuals or entities. Interference with a State's inherently governmental functions may also constitute a violation of State sovereignty, including when undertaken with cyber means.

Uttalandet liknar till innehåll flera andra, mer utförliga uttalanden, t ex det norska, som uttryckligen talar om suveränitet. Vidare hänvisas till Tallinnmanualens regel 4, som allmänt anses utgöra ett solitt uttryck för just den territoriella suveräniteten. De svenska och norska papprena finns tillgängliga på https://cyberpolicyportal.org/. Tallinnmanualen är resultatet av ett kodifikationsprojekt, sponsrat av Natos NATO Cooperative Cyber Defence Centre of Excellence. Se Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

[4] "You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute." Julianne Pepitone, China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper, NBC News (June 25, 2015).

Detta stämmer, men det är s.a.s. bara halva sanningen. I den princip som Tallinnmanualen behandlar på de citerade sidorna står: ”Although peacetime cyber espionage by States does not *per se* violate international law, **the method by which it is carried out might do so**” (s. 168 i Tallinnmanualen; min betoning). Det är just metoden som diskuteras ovan. Det är stor skillnad mellan att bedriva underrättelseinhämtning genom öppna källor respektive genom dataintrång.

Om det är regeringens uppfattning att det är tillåtet att genom sårbarheter etc göra intrång i datorer på andra staters territorium bör den förklara den folkrättsliga grunden för denna uppfattning. Den bör också förklara om det finns några begränsningar, t.ex. vad gäller målen för och syftet med intrången, eller om det är så att varje stat utan vidare får hacka vilken dator som helst i världen för vilket ändamål som helst. Accepterar Sverige att andra länder, i jakt på hädare, dissidenter eller utpressningsobjekt, ger sig tillgång till svenska servrar genom metoder som enligt svensk lag skulle utgöra dataintrång? Vill den svenska lagstiftaren att auktoritära stater får åtkomst till information i Sverige genom lösenord som man kommit över på Darknet eller genom flyktingspionage? Hur ställer man sig till industrispionage mot svenska företag, och finns det trovärdiga argument för att sådan verksamhet är folkrättsstridig om ”vanligt” cyberspionage inte är det?

Andra folkrättsliga aspekter

Utkastet till lagrådsremiss, liksom utredningens betänkanden, behandlar integritetsfrågor, främst utifrån Europadomstolens avgörande i fallet Centrum för Rättvisa mot Sverige (vilket berörs också i det tredje stycket i folkrättsavsnittet). Utredningen borde dock ha gjort en mer fullödig MR-bedömning, inte minst utifrån det faktum att Sverige får anses ha en universell MR-förpliktelse att respektera individers privatliv, oavsett var dessa befinner sig eller deras data kan vara lagrad. Detta remissvar har dock inte fokuserat på den frågan.

En annan fråga som behöver utredas är hur den svenska signalspaningen förhåller sig skyddet för diplomatisk korrespondens m m i Wienkonventionen om diplomatiska förbindelser.

Sammanfattande synpunkter

FRA:s underrättelseinhämtning på främmande datorsystem är sannolikt av stor betydelse för Sveriges säkerhet. Den bör dock vila på laglig grund och vara underbyggd av en solid och transparent analys. Det är anmärkningsvärt att det i betänkandet och i lagrådsremissen inte görs några adekvata folkrättsliga överväganden. Eftersom FRA uppenbarligen sedan lång tid har eftersökt också ”lagrade signaler” på datorsystem i andra länder får man utgå från att det tidigare gjorts analyser av huruvida detta är tillåtet, och dessa analyser bör därför kunna användas i en fördjupad beredning av denna fråga. Innan dessa frågor har utretts på ett professionellt, balanserat och öppet sätt bör något lagförslag i denna del inte läggas fram till Riksdagen.

Remissvaret har på fakultetsnämndens uppdrag beslutats av prodekanus, professor Pernilla Leviner. Yttrandet har beretts av professor Pål Wrange. Föredragande har varit utredare Karolina Alveryd. Yttrandet har expedierats av Juridiska fakultetskansliet.

Pernilla Leviner

Karolina Alveryd

Stockholm University

SCILJ
Stockholm Centre for International Law and Justice

2024-12-02

Remissvar - slutbetänkandet ”Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning” (SOU 2024:59)

Detta yttrande över slutbetänkandet *Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning*, SOU 2024:59, insänds s a s spontant av professor Mark Klamberg (avsnitt 2) och professor Pål Wrange (avsnitt 3). Yttrandet har skrivits som ett led i verksamheten vid Stockholm Centre for International Law and Justice (SCILJ) vid Stockholms universitet, där vi är biträdande föreståndare respektive föreståndare, men det utgör inte ett ställningstagande av SCILJ som sådant, eftersom det inte har funnits tid för styrelsen att behandla yttrandet.

Stockholms universitet har inte anmodats yttra sig över slutbetänkandet och SCILJ fick kännedom om betänkandet genom publicitet i Dagens Nyheter den 31 oktober. Vi noterar, med viss förvåning, att remissen tillställts bara en juridisk institution i Sverige (Umeå) och att ingen juridisk institution stod på sändlistan för det tidigare betänkandet om signalspaning, “Signalspaning i försvarsunderrättelseverksamhet” (SOU 2023:51).

1. Inledning

Slutbetänkandet föreslår en helt ny signalspaningslag i krig och krigsfara, och nuvarande signalspaningslag kommer att gälla bara i fred. Signalspaningslagen i krig upphäver flera tidigare begränsningar; spaning på mottagare och sändare i Sverige tillåts i betydligt högre omfattning än i fred, även gentemot ickemilitära plattformar och aktörer. FRA får också direkttillgång till de fiberoptiska kablarna

som korsar Sveriges gränser. Vidare föreslås signalspaningslagen ändras så att signalspaning fortsättningsvis också ska få omfatta ”lagrade signaler”.

2. Signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara (av Mark Klamberg)

Fortsatt regression och återgång till regeringens förslag från 2007

Sveriges signalspaningslagstiftning har varit föremål för intensiv politisk debatt och granskning av Europadomstolen. Lagstiftningsarbetet har präglats av tvära kast och det finns ett behov av att placera SOU 2024:59 bland dessa kast. Regeringen lade fram två propositioner Prop. 2006/07:46 och Prop. 2006/07:63. När förslagen nådde riksdagen 2008 uppstod en splittring i regeringens riksdagsunderlag. Det ledde till en uppgörelse den 25 september 2008 med 15 ändringar, se sid. 26-27 i Prop. 2008/09:201. Nu aktuellt förslag i SOU 2024:59 innebär att tre av dessa ändringar delvis rullas tillbaka, dvs en regression vid krig och krigsfara tillbaka till regeringens förslag från 2007.

Punkt 2 och 3 i september 2008-överenskommelsen medförde att en domstol skulle inrättas och all signalspaning skulle föregås av tillstånd från denna. 7 § i nu aktuellt förslag om signalspaningslag i krig överlåter detta till befattningshavare vid FRA.

Punkt 4 angav att FRA bara skulle få tillgång till de signalbärare (tidigare benämnt "trafikstråk") som domstolen bestämmer. 9 § i nu aktuellt förslag om signalspaningslag i krig upphäver detta och ger FRA direkttillgång till samverkanspunkter för all kabelkommunikation som korsar Sveriges gränser.[1]

Punkt 5 angav att FRA inte får signalspana mot trafik med både avsändare och mottagare i Sverige. Detta mjukades upp redan när överenskommelsen genomfördes 2009[2] och avlägsnas helt med 5 § i nu aktuellt förslag om signalspaningslag i krig.

Punkterna 11 och 12 angav att en underrättelseskyldighet till enskild införs som skulle försäkras genom Statens inspektion för försvarsunderrättelseverksamheten SIUN. 11 § i nu aktuellt förslag om signalspaningslag i krig upphäver detta.

Tillbakarullningen av september 2008-överenskommelsen började tidigare.

Punkt 1 angav att ändamål för vilka signalspaning får bedrivas preciseras ytterligare och anges i lag, vilket specificerade till 8 ändamål som alla rörde hot mot Sverige och

[1] 9 kap. 30 § Lag (2022:482) om elektronisk kommunikation, tidigare 6 kap. 19 a § Lag (2003:389) om elektronisk kommunikation; Prop. 2006/07:63, sid. 83.
[2] Signalspaningslagen 2a §, andra stycket.

svenska intressen.[3] Med Lag (2021:1173) lades en nionde punkt som anger att signalspaning även får ske avseende företeelser ”som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder”. I samband därmed ändrades även lagstiftningen så att andra stater kan få direktåtkomst till data i FRAs uppgiftssamlingar (databaser).[4]

Punkt 6 angav att FRA får bedriva signalspaning endast på beställning av regeringen, Regeringskansliet och Försvarsmakten eftersom gränsdragningen mot polisens verksamhet uppfattades som oklar. Enligt punkt 7 skulle en utredning tillsättas. Med Lag (2012:801) gavs Säkerhetspolisen och Rikskriminalpolisen (numera Nationella operativa avdelningen i **Polismyndigheten**) rätt att inrikta FRAs signalspaning. Den dåvarande regleringen signalspaning tillämpades på ett sätt som innebar att Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten inte fick tillgång till uppgifter från signalspaning när det gäller företeelser som myndigheterna bedriver en förundersökning om. I samband med antagande av Lag (2019:547) fick nämnda myndigheter rätt ta emot underrättelser med inhämtade uppgifter även om det pågår en förundersökning.[5]

Återstående punkter i överenskommelsen var av marginell betydelse, en del rörde utredningar som skulle tillsättas där allmänheten inte hade någon insyn och resultatet är oklart. Med andra ord: med SOU 2024:59 är tillbakarullningen av september 2008-överenskommelsen till stora delar slutförd.

Underliggande orsaker till återkommande lagändringar

Det synes självklart att FRA ska få signalspana gentemot utländska fientliga militära förband som befinner sig inom svenskt territorium. Samtidigt medges detta redan enligt 2a § andra stycket, andra punkten signalspaningslagen (2008:717) av vilken följer att FRA redan idag får inhämta ”signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.” Detta gäller redan såväl i fredstid som i samband med krig (sid. 105). Fråga uppstår därmed vilket behov och lucka som lagförslaget i denna del söker fylla. Svaret framgår ej tydligt av slutbetänkandet, möjliga ledtrådar är textpassager om ”nya hot mot svenska säkerhetsintressen, samhällsviktiga funktioner, eller underrättelsehot mot svensk känslig information som inte får hamna i främmande makts händer” och ”hybridhot” (sid. 97). Det kan handla om ”fientlig verksamhet … från icke militära plattformar och strukturer [med] utgångspunkt inom exempelvis politiska

[3] Signalspaningslagen 1 §, andra stycket.
[4] 3 kap. 3 § lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt
[5] Prop. 2018/19:96

och diplomatiska, psykologiska och informationsmässiga, underrättelseinhämtande och krigsförberedande åtgärder". (sid. 105)

Jag menar att det finns en underliggande orsak genom den valda lagstiftningstekniken som framtvingar löpande lagändringar, inklusive nu aktuellt förslag. Det handlar om den väldigt breda innebörd som regeringen och lagstiftaren gett åt begreppet "signalspaning". Det omfattar allt från spaning mot radarstationer, fientligt luftvärn, radiovågor, satellitkommunikation, civil internettrafik och med nu aktuellt förslag: lagrade uppgifter i en dator. Vilka kommunikationsformer som egentligen avses är svår att besvara utifrån lagtexten då den endast talar om "signaler", vilket ger lagen en väldigt bred omfattning. Detta kan ske för olika ändamål, allt från fientlig militär verksamhet, underrättelseverksamhet mot främmande makt (ambassadspionage), internationell brottslighet, och terrorism. Allt detta ska regleras med en enda sammanhållen lag, signalspaningslagen. Det sker under parollen "teknikneutralitet"[6], vilket skapar spänningar i hur tillåtande lagstiftningen ska vara och på vilken detaljnivå. Som förklarats tidigare:

> Lagstiftningen som rör signalspaning har samma gemensamma regelverk för underrättelseverksamhet riktad mot 1) främmande väpnade styrkors radar- och luftvärnssystem och 2) organisationer och nätverk för knippade med internationell terrorverksamhet och brottslighet, de senare bland annat i syfte att ge stöd till de brottsbekämpande myndigheterna.
>
> Integritetsintrånget och eventuella rättssäkerhetsförluster gentemot den främmande statens radar- och luftvärnssystem är obefintligt – eftersom allmänhetens kommunikation inte berörs – vilket talar mot detaljerad reglering, medan integritetsintrånget och rättssäkerhetsförluster vid terror och brottsbekämpning är mer påtagliga, vilket talar för en detaljerad och transparent reglering. Signalspaning får dock inte användas i samband med förundersökning. Gemensamma och teknikneutrala regler för dessa två vitt skilda verksamheter kan således leda till att viss verksamhet blir alltför hårt reglerad, medan annan verksamhet blir alltför löst reglerad.[7]

Regeringen och berörd myndighet möter vad de uppfattar som alltför hård reglering av spaning mot främmande makt genom lagförslag om separata regelverk i fred respektive krig. Bieffekten är att verksamheter som förtjänar stram reglering, även i tid av krig och krigsfara, terror och brottsbekämpning dras med i avregleringen.

---

[6] Prop. 2006/07:46, s. 31, 59, 117, 135 (bilaga 1), 194 (bilaga 8).

[7] Mark Klamberg, "Personuppgifter vid brottsbekämpning och försvarsunderrättelseverksamhet" i Fast m.fk. (red.) Röättsinformatik, femte upplagan, 2024, sid. 243.244,

Detta är ett problem då spaning som avser terror och brottsbekämpning även kan beröra och omfatta personer i det omgivande samhället som ej är brottslingar. Sådan underrättelseverksamhet förtjänar stramare reglering.

Alternativa förslag

Jag anser att den tekniska kapacitet som medges genom signalspaning och omfattande inhämtning som rättsligt medges ej är lämpliga i proportionalitetshänseende gentemot kommunikation mellan avsändare och mottagare i Sverige. **Denna** uppfattning förstärks genom att lagförslaget föreslår att signalspaning även ska kunna användas mot lagrade uppgifter (s.k. hackning; se avsnitt 3), dvs FRA kommer i krig eller krigsfara ha rätt att hacka datorer i Sverige utan krav på att dessa datorer används av utlänningar eller kan kopplas till militär verksamhet. Vad gäller verksamhet från icke militära plattformar, däribland politiskt påverkansarbete från annan stat, anser jag det mer lämpligt att sådant hanteras av polis och SÄPO med deras existerande tvångsmedel och den underrättelseinhämtning som de förfogar över. Till detta kommer de uppgifter som utförs av Myndigheten för psykologiskt försvar och Myndigheten för samhällsskydd och beredskap, bl.a. genom användning och användning av öppna källor. Det är ett lämpligare och mer proportionellt sätt att bemöta den lucka som slutbetänkandet tycks peka på.

Från tidigare lagstiftningsarbete samt slutbetänkandet (sid. 52 och 53) framgår det att FRA inhämtar och lagrar stora mängder rådata, däribland trafikdata som ej kan kopplas till något yttre hot och som endast analyseras i efterhand. I Europadomstolens dom i Centrum för Rättvisa mot Sverige medger den svenska regeringen att sökbegreppen (selectors) för att inhämta trafikdata (communications data) är mindre specifika jämfört med de som används för inhämtning av innehåll (content data).[8] Med mindre specifika sökbegrepp omfattas en större andel av den samlade kommunikationen. Med hänsyn till hur modern elektronisk kommunikation fungerar så kan data mellan avsändare och mottagare som båda befinner sig i Sverige likväl korsa landets gränser och därmed ske i de kablar som slutbetänkandet nu föreslår att FRA ska få direkttillgång till. Inhämtningen av trafikdata som hänför sig till avsändare och mottagare som båda befinner sig i Sverige har med nuvarande lagstiftning begränsats. Med lagförslaget avlägsnas ännu en **barriär** och det framstår som att lagförslaget kommer kunna medge att FRA kan inhämta och lagra all trafikdata som kommuniceras genom de aktuella signalbärarna, även sådan som

[8] Centrum för Rättvisa mot Sverige, Europodomstolen, ansökan 35252/08, dom den 25 maj 2021, para. 220.

hänför sig till avsändare och mottagare som båda befinner sig i Sverige och som saknar koppling till yttre hot.

Ovanstående redogörelse kan framstå som teknisk och svårtillgänglig. För att förklara det med andra ord och exempel: när slutbetänkandet föreslår att tillåta spaning mot mottagare och avsändare i Sverige samt att ge FRA direkttillgång till digitala kommunikationsflöden bör vi jämföra med det tillstånd och verksamhet som rådde innan signalspaningslagen trädde ikraft den 1 januari 2009. I ett internt FRA-dokument, publicerat av SVT den 16 juni 2008 och senare delvis utlämnat som allmän handling, anges följande: ”FRA arbetar på så sätt all tillgänglig kommunikation lagras. I efterhand görs sökningar i den trafiken … hanteringen av trafikdata skiljer sig från hanteringen av inhämtat innehåll”.[9] Nu aktuellt slutbetänkande kommer i stora delar upphäva den överenskommelse som regeringspartierna träffade hösten 2008, som skedde mot bakgrund av SVTs avslöjande och vars bärande delar var att begränsa FRAs tillgång till signalbärare och förbud mot att inhämta kommunikation mellan avsändare och mottagare i Sverige, se punkterna 4 och 5 i överenskommelsen.[10] Syftet var bl.a. att förhindra omfattande inhämtning och lagring av rådata/trafikdata, se punkt 14 i överenskommelsen. Slutbetänkandet riskerar en återgång till den omfattande inhämtning och lagring som FRA bedrev före det att signalspaningslagen trädde ikraft 2009.

Slutbetänkandets förslag framstår som alltför omfattande och genomgripande i proportionalitetshänseende. Behovet av skyndsamhet i krig eller krigsfara är likväl ett legitimt intresse. Det leder fram till två alternativa förslag.

Det första alternativet utgår från slutbetänkandets förslag att ha en lagstiftning för fred och en annan i krig. Vad avser signalspaning i krig bör lagändringen begränsas till att ge FRA rådighet över signalbärarna, men ej utvidgad rätt att inhämta signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Vidare, signalspaningslagen i krig ska ej tillämpas för ”strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet”.[11] Istället ska signalspaningslagen i fred gälla för denna form av hot. För det fall främmande statsmakt ägnar sig åt verksamhet i en gråzon så får det hänföras till ”främmande

[9] FRA, ‘Frågor & svar’, 14 mars 2007; Struwe, Filip, ‘FRA lagrar svenska telesamtal och mejl, (Sveriges Television, 16 juni 2008.

[10] Förstärkt integritetsskydd vid signalspaning, Prop. 2008/09:201, sid. 26-27.

[11] 1 § andra stycket, punkt 3, signalspaningslagen.

makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik" där signalspaningslagen i krig gäller.[12]

Det andra alternativet är mer genomgripande genom att den förkastar förutsättningen att lagstiftningen ska vara "teknikneutral" och sammanhållen. Istället för en uppdelning i två separata lagar som skiljer på fred och krig, så ska skiljelinjen gå mellan lagstiftning riktad mot främmande statsmakt å ena sidan och lagstiftning som rör bekämpning av brott och terror å andra sidan. Den förstnämnda lagstiftningen kan vara tillåtande på samma sätt som SOU 2024:59 föreslår medan den sistnämnda skulle vara hårdare begränsad på samma sätt som existerande lagstiftning för tvångsmedel och underrättelseinhämtning avseende rent svenska förhållanden.

En mindre justering avser förslaget till ny § 2b i signalspaningslagen, som upphäver förbudet mot inhämtning av kommunikation mellan avsändare och mottagare i Sverige i brådskande situationer. Det handlar om situationer som hamnar i gränslandet mellan FRAs nuvarande rättsliga befogenheter å ena sidan, polisens tekniska förmågor och rättsliga befogenheter å andra sidan. Slutbetänkandet söker utnyttja FRAs tekniska förmågor ytterligare. En möjlig risk är att § 2b används för att kringgå ordinarie regler för övervakning och avlyssning som polis förfogar över. Det kan i sin tur kan få konsekvenser för den enskildes möjlighet att få tillgång till information beträffande de själva, där polisen har större skyldigheter gentemot den enskilde jämfört med FRAs mycket begränsade skyldigheter, med andra ord en fråga om rättssäkerhet. Därmed kan det vara motiverat i lagförslaget till ny § 2b tillföra krav att polisens ordinarie medel ej är tillgängliga utöver kravet på att det ska vara en "brådskande situation".

3. FRA ges explicit rätt att inhämta "lagrade signaler" (av Pål Wrange)

Utredningen föreslår en avsevärd förändring av FRA:s lagstadgade uppdrag och mandat genom ett tillägg av nio ord i 1 § signalspaningslagen (här kursiverade):

> I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer

[12] 1 § andra stycket, punkt 8, signalspaningslagen.

(signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning, *oavsett om signalerna är under förmedling eller är lagrade*. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Som ska förklaras nedan innebär förslaget att FRA ges explicit rätt att hacka sig in i datorsystem i andra länder, vilket reser ett antal frågor. Den första är huruvida detta utgör en förändring av FRA:s uppdrag, och om det i så fall är en betydande förändring som förtjänar noggranna överväganden.

Utgör förslaget en förändring eller ett förtydligande av vad som redan gäller?

Förslaget sägs vara ett ”förtydligande” som kodifierar den praxis som redan sker, efter tillstånd från Försvarsunderrättelsedomstolen och under insyn av Siun (s 135; även 136 och 241). Det utgör alltså “ett förtydligande i lag” som ”bidrar till att tydliggöra inhämtningens omfattning” (s 229). För att ett ny lagformulering ska kunna sägas utgöra ett förtydligande av en befintlig lag snarare än en lagändring krävs emellertid att en rimlig tolkning av den befintliga lagen kan omfatta också den förändrade lydelse. Det förefaller inte vara fallet.

Med signalspaning menas i vedertaget språkbruk att man upptar signaler från etern eller från kablar. Nationalencyklopedin definierar det på följande, något föråldrade[13] sätt:

> **signalspaning,** verksamhet för att genom avlyssning, lägesbestämning och identifiering av radio- eller radarsignaler (eller sändare) eller annan avsiktlig eller oavsiktlig elektromagnetisk strålning skaffa information om en (potentiell) motståndares tekniska och operativa resurser och dispositioner.

Wikipedias definition är den följande:

> **Signalspaning** (förkortas ofta **SIGINT** från engelskans *signals intelligence*) innebär att man genom avlyssning, pejling m.m. utforskar och övervakar data- och/eller teletrafik och på så vis inhämtar underrättelser.

Enligt SAOL är en signal ”ton, ljus-blink e.d. med visst budskap”, alltså något som förmedlas från en avsändare till en eller flera mottagare. ” I vardaglig svenska förefaller det alltså främmande att med termen ”signaler” mena all information som finns lagrad och än mer främmande att med ”signalspaning” mena något annat än undersökande av signaler som befinner sig i trafik från A till B (eller möjligen

[13] Definitionen har uppenbarligen inte tagit hänsyn till lagändringen år 2008.

signaler som sänds ut från maskiner utan att utgöra information i vardaglig mening). Inte ens FRA:s egen förklaring leder tankarna åt lagrad data.[14]

Detta är också det bestämda intryck som ges i den befintliga lagen. I 1 § beskrivs verksamheten som så att FRA får ”inhämta signaler i elektronisk form vid signalspaning,” Enligt 2 § får inhämtning av signaler i tråd endast avse signaler som ”*förs över* Sveriges gräns i tråd som ägs av en operatör”, och av 2 a § framgår att signaler ”*mellan* en avsändare och mottagare som båda befinner sig i Sverige” inte får inhämtas (mina kursiveringar).

Det kan i princip tänkas att avsikten med förändringen är att det som ska eftersökas bara är lagrade meddelanden, dvs lagrade mejl, chattmeddelanden och liknande. I så fall borde det ha klargjorts i lagen eller i vart fall i förarbeten. I ljuset av det som är känt om FRA:s verkliga aktiviteter förefaller det emellertid inte sannolikt.[15]

Oavsett om det bara handlar om lagrade meddelanden eller om all lagrad information och data så utgör den verksamhet som avses med de tillagda nio orden det som i brottsbalken kallas dataintrång, i svensk straffprocessrätt benämns hemlig dataavläsning, internationellt kallas ”cyber espionage” och på vardaglig svenska kallas hackning. Det som nu föreslås är alltså artskilt från det som beskrivs i den befintliga lagen, och förslaget innebär därför en avsevärd utvidgning av FRA:s lagstadgade mandat.

Utredningens argumentation för att detta bara handlar om ett ”förtydligande” är mycket svår att förstå. På flera ställen hävdas att FRA:s uppdrag och rätt att utföra underrättelseverksamhet i ”lagrade signaler” följer av de tidigare förarbetena (s 135). På s 241 sägs följande:

> Av tidigare förarbeten framgår att möjligheten att inhämta signaler i elektronisk form inte är knuten till var signalerna befinner sig. Därmed kan inhämtning ske oavsett om signalerna befinner sig i etern eller i kabel (dvs. är trådburen) eller någon annan stans (se prop. 2006/07:63 s. 36.).

Den citerade s 36 innehåller emellertid bara en redogörelse för vad remissinstanser sagt om en annan fråga, och hänvisningen måste utgöra ett misstag. En något fylligare argumentation finns på s 132-133. Utredningen tar här sitt avstamp i remissvaret från Kustbevakningen till Försvarsdepartementets promemoria (Ds 2005:30) där remissinstansen ”anfört att begreppet signaler i elektronisk form utgör en begränsning eftersom signalerna kan överföras på annat sätt än elektroniskt, t.ex.

---

[14] FRA, Vad är signalspaning, Signalspaning och kryptering - FRA.

[15] Se t ex Hugh Eakin, The Swedish Kings of Cyberwar, The New York Review of Books, January 19, 2017.

genom fiberoptik, och det kan ifrågasättas om den aktuella bestämmelsen borde göras inriktad på signaler eller uppgifter snarare än på teknik för överförande" (prop. 2006/07:63 s. 70). Utredningen fortsätter:

> Regeringen anförde att fokus bör vara på vad som får inhämtas, snarare än i vilket system signalerna överförs. Med signaler i elektronisk form avses alla former av signaler som överförs bland annat med hjälp av elektromagnetiska vågor. Det saknades därför enligt regeringens uppfattning anledning att gå ifrån den i promemorian föreslagna lydelsen.[9] I författningskommentaren angav regeringen vidare att möjligheten att inhämta signaler i elektronisk form inte är knuten till var signalerna befinner sig. Därmed kan inhämtning ske oavsett om signalerna befinner sig i etern eller i kabel (dvs. är trådburen) eller någon annan stans.[10] Det kan exempelvis vara fråga om signaler som överförs via satellit eller signaler som är lagrade i nätverksansluten utrustning, i såväl mjuk- som hårdvara. Det senare, vilket Försvarsberedningen beskrivit som nätverksinhämtning, syftar till att kartlägga och få åtkomst till information i informationssystem, datorer eller nätverk av dessa.[11] All digital information utgörs således av signaler i elektronisk form. (133)

Fotnot 9 hänvisar till prop. 2006/07:63 s. 70 f. Där står emellertid inget om signaler som är lagrade. För övrigt handlar resonemanget i anslutning till denna fotnot om signaler som ”överförs”, inte om signaler som lagras. Fotnot 10 hänvisar till prop. 2006/07:63 s. 137. Där står inte heller något om signaler som är lagrade. Ordet ”lagra” förekommer för övrigt i propositionen bara vad gäller FRA:s lagring, inte vad gäller ”signaler” som lagrats av andra. Fotnot 11 hänvisar till Försvarsberedningens rapport Ds 2019:8 s. 253, som är det enda citerade ställe som pekar mot att det kan vara fråga om eftersökning av lagrad information. Där står följande:

> Underrättelseinhämtning genom nätverksinhämtning syftar till att kartlägga och få åtkomst till en motståndares information, informationssystem, datorer eller nätverk av dessa. En viktig del av nätverksinhämtning är att kartlägga sårbarheter i motståndares system, vilket är en förutsättning för att kunna genomföra offensiva operationer.

Här kan först noteras att det inte i klarspråk anges att det är fråga om verksamhet också i fred (även om man kan anta att så är fallet). Betydligt viktigare är emellertid att detta rapportavsnitt inte utgör ett förarbetsuttalande. Enligt sedan mycket lång tid vedertagen uppfattning ska rättstillämparen ta hänsyn till förarbetena till en lag, under förutsättning att förarbetsuttalandena görs under lagstiftningsprocessen, vilken i allmänhet utgörs av utredning, remissförfarande, lagrådsremiss, proposition

och utskottsbehandling, där olika samhällsintressen och politiska uppfattningar kan brytas mot varandra och vägas. Vad Försvarsberedningen skriver i en rapport år 2019 har alltså ingen relevans för hur en lag från 2008 ska tolkas.

Utredningen skriver att det är ”av stor betydelse för allmänhetens förtroende för signalspaning i försvarsunderrättelseverksamhet att verksamhetens omfattning är klar och tydlig” (s 136). Den bild som framträder är att den verksamhet som synbarligen bedrivits inte bara strider mot lagens bokstav utan dessutom mot lagens förarbeten. Att det s a s varit en offentlig hemlighet att FRA under lång tid ägnat sig åt vad man kallar ”aktiv signalspaning”, och att detta med största sannolikhet har varit känt av flera andra svenska offentliga institutioner, förändrar inte den saken.

Det som är relevant för detta remissyttrande är att den verksamhet som avses med lagförändringen aldrig varit föremål för den omsorgsfulla beredning som krävs i svensk lagstiftningsprocess, och som också delvis följer av Regeringsformens 7 kapitel 2 §. Enligt detta stadgande gäller att ”[v]id beredningen av regeringsärenden ska behövliga upplysningar och yttranden inhämtas från berörda myndigheter. … Även sammanslutningar och enskilda ska i den omfattning som behövs ges möjlighet att yttra sig.” Eftersom det under förberedelserna för 2008 år lag inte hade diskuterats huruvida FRA skulle få möjlighet att genomsöka lagrad information var det inte heller möjligt för myndigheter, sammanslutningar och enskilda att yttra sig om den saken.

När hemlig dataavläsning genom lagen 2020:62 infördes som ett processrättsligt tvångsmedel utreddes detta i ett betänkande på sammanlagt 689 sidor. I denna utredning diskuteras motsvarande fråga på sju sidor, vilka ger det missvisande intrycket att förändringen snarast är en formalitet. De följande styckena kommer att förklara varför noggranna överväganden nu behövs.

Inhämtningsförbud beträffande signaler som lagras i Sverige

Som en följdändring till utvidgningen till lagrad information skrivs följande:

> Enligt 2 a § signalspaningslagen får inhämtning inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Med hänsyn till det förtydligande som utredningen föreslår finns det, enligt utredningen, en risk för att 2 a § signalspaningslagen i sin nuvarande ordalydelse inte omfattar signaler som lagras. Det är inte utredningens avsikt med förslaget. (s 137)
>
> [D]et bör därför framgå att inhämtningsförbudet även gäller signaler som är lagrade i Sverige. (s 138)

I lagförslaget skrivs följande, med ändringen kursiverad:

> 2 a § Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete. … *Första stycket … tillämpas även på signaler som lagras i Sverige*.

Enligt min uppfattning är det inte klart vad som menas. Förslaget kan förstås på (mins) två sätt.

1. Det finns ett generellt förbud mot inhämtning av ”signaler” som lagras i Sverige, och detta förbud är oberoende av förbudet i den första meningen mot inhämtning av ”signaler mellan en avsändare och mottagare som båda befinner sig i Sverige”. Om *någon* av dessa två omständigheter är för handen får den lagrade signalen alltså inte inhämtas (dvs de utgör alternativa rekvisit i juridiska termer). Om avsikten är att göra avgränsningen vad gäller lagrad information kongruent med avgränsningen avseende meddelanden, dvs att personer i Sverige ska skyddas, missas syftet med denna tolkning. Platsen för lagring av information är inte beroende av platsen där personen befinner sig. ”Lagrade signaler” (som trafikdata, abonnentdata och innehåll) från personen X i Sverige kan lagras i olika länder, beroende på hur den aktuella tjänsteleverantören har valt att lagra dem. Omvänt gäller förstås att ”lagrade signaler” som avser en i utlandet bosatt person kan lagras i någon av de många serverhallar som finns i Sverige för leverantörer som Amazon och Facebook. Denna avgränsning förefaller alltså inte funktionell, oavsett om syftet är att skydda invånare i Sverige eller att fånga in så många utländska hot som möjligt.

2. Den andra förståelsen är att rekvisitet ”signaler som lagras i Sverige” är ett villkor *utöver* begränsningen avseende avsändare och mottagare (ett kumulativt rekvisit för att inhämtning ska vara förbjuden). Detta betyder i så fall att lagrade signaler inte får inhämtas om de utgör signaler mellan en avsändare och mottagare som båda befinner sig i Sverige som *dessutom* är lagrade i Sverige. En konsekvens därav är att vad gäller lagrade signaler så förbjuds inhämtning bara om båda villkoren är uppfyllda, dvs att det handlar om ”signaler mellan en avsändare och mottagare som båda befinner sig i Sverige” vilka ”lagras i Sverige”. Det behöver inte påpekas att förbudet i så fall är tämligen begränsat, eftersom alla signaler

mellan personer i Sverige som lagras utomlands blir tillgängliga.

Oavsett vilken förståelse som är avsedd bör det klargöras vad som menas, samt bör det förklaras hur det avsedda förslaget ska ses från såväl effektivitets- som integritetsperspektiv.

Rätten att vidta ”tekniska åtgärder”

Utredningen föreslår att 2 § kompletteras med följande skrivning:

> Vid inhämtning enligt 1 och 1 a §§ av signaler i elektronisk form får signalspaningsmyndigheten vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtningen.

I en mening förklaras vad som menas med ”tekniska åtgärder”, nämligen att ”Försvarets radioanstalt [kan] behöva utnyttja tekniska sårbarheter, förbiseenden och inbyggda åtkomstmöjligheter i nätverksansluten utrustning” (s 136 och 242). Detta är i stort sett vad som i dagligt språk kallas hackning.

För att förtydliga vad det handlar om: Med ”sårbarheter” menas – mycket starkt förenklat -- buggar i programvara.[16] Buggar kan utnyttjas också av kriminella, kan vara till salu på Darknet och kan läcka från säkerhetsmyndigheter. Att utnyttja sårbarheter kan medföra svåra etiska problem. Ska en säkerhetstjänst som känner till en sårbarhet i t ex Windows 11 behålla den för sig själv för att kunna utnyttja den för sina behov eller ska man underrätta tillverkaren, t ex Microsoft, så att de kan täppa till luckan? Exemplet Shadow brokers[17] visar att detta är frågor av potentiellt stor betydelse för allmänheten. De nämns dock inte i utredningen.

Med förbiseenden avses sannolikt ”phishing”, dvs att någon av förbiseende klickar på en länk som den inte borde klicka på, varpå ett spionprogram eller liknande installeras, och det kan förmodligen också innefatta bristfällig hantering av lösenord. Med ”inbyggda åtkomstmöjligheter” kan menas att den som säljer en hård- eller mjukvara medvetet lagt in en så kallad bakdörr eller liknande. När så sker är det givetvis på uppdrag av en underrättelsetjänst. Riskerna för att bakdörrar skulle kunna utnyttjas av kriminella diskuteras inte.

---

[16] Att det finns en n sårbarhet behöver inte betyda att det är något fel på programvaran med avsedd användning (dvs vad vi vanligen betecknar som bugg), men det kan betyda att någon har hittat ett sätt att genom att komma runt den avsedda användningen ta sig in i systemet.

[17] En hacker-grupp med detta namn lyckades bl a komma åt amerikanska NSA:s EternalBlue-mjukvara, vilken sedan användes i två av de största hackerattackerna under senare år: NotPetya (sannolikt från Ryssland) och WannaCry (sannolikt från Nordkorea).

Folkrättsliga aspekter

Diskussionen om ”tekniska åtgärder” leder in på de synnerligen viktiga folkrättsliga aspekterna, särskilt frågan om Sverige, inklusive FRA, har förpliktelser att respektera vad som på FRA:s webbsida kallas den digitala territorialgränsen. Även om det – trots vad som anförts ovan -- vore så att lagförslaget inte utgör en egentlig förändring så borde utredningen ha tagit upp detta, eftersom det (såvitt kan utrönas) inte gjordes under lagstiftningsprocessen inför 2008 års lag. När FRAs dåvarande generaldirektör hördes av riksdagens försvarsutskott den 13 maj 2008 fick han frågan om den föreslagna lagstiftningen skulle medge aktiv signalspaning (hackning) vilket han tillbakavisade (bilaga till protokoll, utskottssammanträde 2007/08:36).

Traditionell signalspaning har utövats inom en stats gränser eller på (eller över) internationellt vatten. Den spanande staten har agerat utan att direkt kränka en annan stats suveränitet. (Däremot kan den spanande staten ha gjort intrång som påverkar individers rätt till privatliv.) När signalspaningen utsträcktes till trådbundna signaler hände inget avgörande från ett suveränitetsperspektiv, under förutsättning att spaningen inte utförs på andra staters territorium. (Däremot kan ITU-regler vara relevanta, men det utreddes säkert när signalspaningslagen vidgades till att tillåta signalspaning i ”tråd”.)

Att ”signalspana” i datorsystem på andra staters territorium är en helt annan sak. Internationellt har det sedan 1998 pågått såväl mellanstatliga som akademiska diskussioner om huruvida territoriell suveränitet gäller i ”cyberrymden”. Sedan 2013 är det en vedertagen uppfattning att folkrätten i stort gäller också i cyberrymden, men frågan om territoriell suveränitet är fortsatt kontroversiell. Ett antal stater, däribland Sverige, har avgivit positionspapper där man angett sina synpunkter på denna och andra frågor. Det finns idag också en ganska omfattande internationell juridisk litteratur i ämnet.

I den mest kända folkrättsliga monografin, Oppenheim’s International law, sägs att “[a] state is not allowed to send its troops, its warships, or its police forces into or through foreign territory, or its aircraft over it, or to carry out official investigations on foreign territory or to let its agents conduct clandestine operations there, or to exercise an act of administration or jurisdiction on foreign territory, without permission.”[18]

[18] Sir Robert Jennings (ed.), Arthur Watts KCMG QC (ed.), Oppenheim's International Law: Volume 1 Peace (9th Edition, 1992, Oxford University Press) § 119.

I Oppenheimcitatet görs ingen skillnad mellan intrång för brottsbekämpning, för nationell säkerhet eller för andra ändamål. Inom internationell brottsbekämpning är det en vitt spridd – men inte enhällig -- uppfattning att eftersökning av uppgifter på datorsystem i andra stater inte är tillåten. Det var också den svenska uppfattningen, i vart fall fram tills Högsta domstolens beslut i målet ”Den okända lagringsplatsen”.[19] Frågan om extraterritoriella polisiära undersökningsåtgärder, som genomsökning av datorsystem i andra länder, har utretts i en SOU från 2023 (om än i många stycken bristfälligt).[20]

Den mest omdebatterade frågan internationellt är hur den traditionella regel som uttrycks i Oppenheim (och som ingen bestrider i princip) ska förstås vad gäller olika cyberåtgärder. Frankrike, t ex, har en strikt syn och menar att ”[e]very non-authorised penetration by a state actors into French systems …may constitute, at a minimum, a violation of sovereignty”. Andra stater, som t ex Nederländerna, har en liberalare syn medan USA och Storbritannien (men inga andra stater) anser att den territoriella suveräniteten inte gäller i ”cyberrymden” över huvud taget.[21] I Sveriges positionspapper från 2022 sägs att ”States … have an obligation to respect the sovereignty of other States.”[22] Det kan antas att detta positionspapper har beretts på sedvanligt sätt, dvs inklusive konsultationer med Försvarsdepartementet.

Förutom de rent juridiska aspekterna av dessa frågor finns det också synnerligen viktiga policyaspekter, som inte berörs i utredningen, inte minst vad gäller andra staters reaktioner på svenskt agerande eller andra staters reciproka agerande. T ex kan svenska inhämtningsåtgärder som i enlighet med utredningens förslag sker på datorsystem i andra länder bedömas som dataintrång eller värre i dessa länder,

---

[19] SOU 2017:89. HD-beslutet har referens NJA 2023 s. 231.

[20] SOU 2023:22 ss 465 ff. Juridiska fakultetens vid Stockholms universitet mycket kritiska remissvar återfinns på Stockholms universitet (juridiska fakulteten), ss 13-17-

[21] Däremot menar man att andra regler gäller, t ex förbudet mot våldsanvändning.

[22] Vidare:

> In general, Sweden is of the view that violations of sovereignty may arise from cyber operations that result in damage or loss of functionality. Altering and interfering with data without causing physical harm may also violate sovereignty. Such acts include those directed against cyber infrastructure belonging to private individuals or entities. Interference with a State’s inherently governmental functions may also constitute a violation of State sovereignty, including when undertaken with cyber means.

Uttalandet liknar till innehåll flera andra, mer utförliga uttalanden, t ex det norska, som uttryckligen talar om suveränitet. Vidare hänvisas till Tallinnmanualens regel 4, som allmänt anses utgöra ett solitt uttryck för just den territoriella suveräniteten. De svenska och norska papprena finns tillgängliga på https://cyberpolicyportal.org/. Tallinnmanualen är resultatet av ett kodifikationsprojekt, sponsrat av Natos NATO Cooperative Cyber Defence Centre of Excellence. Se Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

vilket i så fall kan utsätta FRA-anställda för risker, inte bara vid besök i dessa stater utan indirekt genom utlämning från stater som samarbetar med dessa stater.

Vidare måste man överväga hur den regel som FRA synbarligen tillämpar, nämligen att det är tillåtet att bryta sig in datorsystem i andra länder, har för effekt för Sverige i an ”whole of society”-analys. Det är uppenbart att denna regeltolkning har tjänat Sverige väl i så måtto att den har gett FRA möjlighet att inhämta information som är viktig för Sveriges säkerhet, men den fråga som måste ställas och diskuteras är vilka följder den kan få för andra svenska intressen. Accepterar Sverige att andra länder, i jakt på hädare, dissidenter eller utpressningsobjekt, ger sig tillgång till svenska servrar genom metoder som enligt svensk lag skulle utgöra dataintrång (eller värre)? Vill den svenska lagstiftaren att auktoritära stater får åtkomst till information i Sverige genom lösenord som man kommit över på Darknet eller genom flyktingspionage? Hur ställer man sig till industrispionage mot svenska företag, och finns det trovärdiga argument för att sådan verksamhet är folkrättsstridig om ”vanligt” cyberspionage inte är det? När det år 2015 avslöjades att Kina, i den s k OPM-hacken, hade skaffat sig tillgång till information om 22 miljoner federalt anställda personer i USA (en del av vilken information var synnerligen känslig), kunde den amerikanska underrättelsechefen James Clapper inte säga annat än att han gratulerade kineserna (och skulle göra likadant om han kunde), eftersom detta agerande, enligt amerikanskt synsätt, inte bröt mot folkrätten.[23]

Mänskliga rättighetsaspekter (MR-aspekter) m m

Utredningens betänkande, liksom det tidigare betänkandet från 2023, behandlar integritetsfrågor, främst utifrån Europadomstolens avgörande i fallet Centrum för Rättvisa mot Sverige. Utredningen borde dock ha gjort en mer fullödig MR-bedömning, inte minst utifrån det faktum att Sverige får anses ha en universell MR-förpliktelse att respektera individers privatliv, oavsett var dessa befinner sig eller deras data kan vara lagrad. Detta remissvar har dock inte fokuserat på den frågan.

En annan fråga som behöver utredas är hur den svenska signalspaningen förhåller sig skyddet för diplomatisk korrespondens m m i Wienkonventionen om diplomatiska förbindelser. Denna fråga verkar inte ha berörts i propositionen från 2007.

---

[23] ”You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute.” Julianne Pepitone, China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper, NBC News (June 25, 2015).

Sammanfattande synpunkter rörande inhämtning av ”lagrade signaler”

FRA:s underrättelseinhämtning på främmande datorsystem är sannolikt av stor betydelse för Sveriges säkerhet. Den bör dock vila på laglig grund och vara underbyggd av en solid och transparent analys. Det är synnerligen anmärkningsvärt att det inte i denna utredning, och såvitt kan bedömas inte heller tidigare, görs några som helst folkrättsliga överväganden. Förutom att det rimmar illa med den traditionella svenska linjen att sätta folkrätten mycket högt[24] innebär det också att utredningen försummar det viktiga svenska policy-intresset att påverka folkrättens utveckling i ”cyberrymden”, genom konkret handlande, genom lagstiftning och genom rättsliga analyser. En särskilt viktig aspekt är reciprocitetsprincipen, dvs att en stat inte kan förvänta sig att bli behandlad efter andra regler än de som den själv tillämpar. Eftersom FRA uppenbarligen sedan lång tid har eftersökt också ”lagrade signaler” på datorsystem i andra får man utgå från att FRA och/eller Försvarsdepartementet tidigare gjort interna analyser av huruvida detta är tillåtet, och dessa analyser bör därför kunna användas i en fördjupad beredning av denna fråga. Innan dessa frågor har utretts på ett professionellt, balanserat och öppet sätt bör något lagförslag inte föreläggas riksdagen i denna del.

4. Slutord

I detta yttrande har det framförts invändningar mot och synpunkter på delar av förslaget. Vad gäller förslaget att signalspaning också ska få ske i lagrad information har det därtill hävdats att beredningskravet inte är uppfyllt, och att lagförslaget i denna del inte kan föreläggas Riksdagen med mindre än att utredningen kompletteras betydligt.

Mark Klamberg
Professor i folkrätt

Pål Wrange
Professor i folkrätt

[24] I årets utrikesdeklaration sägs att det ”[f]ör Sveriges säkerhet och stabiliteten i omvärlden är … avgörande att den regelbaserade världsordningen, folkrätten och respekten för FN-stadgan upprätthålls.” Utrikesdeklarationen, 14 februari 2024. Utrikesdeklarationen 2024 - Regeringen.se