Stockholms universitet

2023-10-31 Dnr SU FV-2740-23

Juridiska fakultetskansliet Justitiedepartementet

Remiss av betänkandet Datalagring och åtkomst till elektronisk information

Juridiska fakultetsnämnden har fått möjlighet att yttra sig över betänkandet *Datalagring och åtkomst till elektronisk information (SOU 2023:22).*

1. Sammanfattning

• Juridiska fakultetsnämnden tillstyrker att en teknikanpassning av lagstiftningen införs, vilken innebär att nummeroberoende interpersonella kommunikationstjänster (Noik) inkluderas. Icke desto mindre finns det anledning att befara att lagstiftningen inte kommer att kunna verkställas på det sätt som avses, beroende på att en betydande del av leverantörerna av Noik har sitt säte utanför Sverige och EU.

• Juridiska fakultetsnämnden bedömer att de nya krav på lagringsåtgärder som föreslås i form av nationell säkerhetslagring, geografiskt riktad lagring och utökad riktad lagring, behöver bli föremål för ytterligare utredning och analys. Detta gäller i synnerhet proportionaliteten i åtgärderna samt utformningen av de förfaranden som föreslås. Juridiska fakultetsnämnden kan därför inte tillstyrka dessa förslag i sin nuvarande form. Det ska också påpekas att de nya lagringsåtgärderna reser komplexa frågor som skulle behöva belysas i ett multidisciplinärt perspektiv.

• Förslaget rörande exekutiv jurisdiktion behöver enligt Juridiska fakultetsnämnden bli föremål för en ny utredning och analys rörande de folkrättsliga förutsättningarna och kan därför inte tillstyrkas. Flera oklarheter behöver klargöras, däribland vad som kan anses utgöra ett mer än obetydligt intrång i en annan stats suveränitet.

• Förslaget får konsekvenser för företagen i form av ökade kostnader och konkurrensnackdelar. Utredningen föreslår att den kostnadsfördelningsmodell som tidigare använts består. Juridiska fakultetsnämnden finner emellertid att det inte är förenligt med krav på likabehandling att bibehålla kostnadsfördelningsmodellen, då företag i andra liknande situationer, såsom t.ex. gäller på mervärdesskatteområdet, inte får ersättning för sin lagfästa skyldighet att driva in skatt till staten. Förslaget avstyrkes.

Juridiska fakultetsnämnden

Stockholms universitet
106 91 Stockholm

Besöksadress:
Universitetsvägen 10 A

Telefon: 08 16 44 89
E-post: sandra.persson@juridicum.su.se

2. Övergripande synpunkter på förslaget

Den informationstekniska utvecklingen fortsätter i snabb takt. Det allmänna som det nationella säkerhetsläget bedöms ha påtagligt försämrats. Polismyndigheter och underrättelsetjänster måste göra omställningar i arbetet och beredas nya förutsättningar för att kunna utföra sina uppgifter[1].

Ett flertal nya tvångsåtgärder har införts som ett led i detta, såsom genom lagen (2020:62) om hemlig dataavläsning. På motsatt sida av lagen används nya informationstekniska verktyg såväl av antagonister till Sverige som av grovt kriminella nätverk, vilket innebär stora utmaningar för brottsbekämpningen.

Hotbilderna tornar upp sig i det splittrade medielandskapet, vilka kan vara mer eller mindre väl belagda, med ökad kollektiv oro och behov av politisk handling som följd. Jakten på effektiva motmedel i form av nya tvångsmedel och utökade åtgärder för massövervakning innebär emellertid risker för rättssäkerheten, demokratin och säkerställandet av de mänskliga rättigheterna, särskilt skyddet för den personliga integriteten, vilket kan få allvarliga konsekvenser för samhället på sikt.[2] Proportionalitet är ledstjärnan enligt EU-domstolens och Europadomstolens praxis, så även i Datalagringsutredningens betänkande. Frågan är emellertid hur balansen mellan rättssäkerhet och effektivitet ska ske i det nuvarande läget som också kan vara hållbart på sikt.

Teknikanpassning

Utredningens förslag är delvis ett svar på behovet av en nödvändig teknikanpassning av lagstiftningen om elektronisk kommunikation till nya kommunikationsformer, i synnerhet s.k. OTT-tjänster (Over the Top), även benämnt nummeroberoende interpersonella kommunikationstjänster (Noik). Härefter hänvisas till Noik.

Detta innebär förvisso en utvidgning av skyldigheterna att lagra och tillhandahålla data om elektronisk kommunikation för statens och de brottsbekämpande myndigheternas räkning, men kan samtidigt framstå som legitim eftersom många individer väljer att kommunicera via Noik framför andra tjänster i allt större utsträckning. En följd av detta är också att anpassningsskyldigheten för tjänsteleverantörerna enligt lagen (2022:482) om elektronisk kommunikation (LEK) måste moderniseras så att de inkluderar Noik.

Det föreligger emellertid en inte oansenlig risk att förslaget rörande Noik inte får den effekt som eftersträvas eftersom de företag som tillhandahåller dessa tjänster till stor del är belägna utanför EU och det inte är självklart att de kommer att kunna hörsamma lagrings- och anpassningskrav från svenska myndigheter på samma sätt som svenska företag.[3] Frågan behandlas vidare under avsnittet om exekutiv jurisdiktion.

---

[1] Ett exempel på detta är att underrättelseinhämtningen som tidigare skedde i en mer sluten värld, i dessa tider av s.k. ”big data”, i allt större utsträckning präglas av informationsinhämtning från öppna källor, Open source intelligence. Se Friborg, Nadja & Koraeus, Mats, AI och framtidens underrättelsetjänst i Akenine, Daniel & Stier, Johan (red.), Människor och AI – Fem år senare, AddAI (e-bok) 2023, s. 33 f.

[2] Jfr. Flyghed, Janne, Normalisering av det exceptionella – ett led i den sociala kontrollens expansion i Estrada, Felipe et al., I rättsstatens sprickor – En vänbok till Janne Flyghed, Kriminologiska institutionen, Stockholms universitet, Stockholm 2021, s. 83-113.

[3] Daskal beskriver den komplicerade process som detta kan innebära i Daskal, Jennifer, Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, Journal of National Security Law and Policy, vol. 8 nr. 3, 2017 s. 474 f.

Nya lagringskrav

Datalagringsutredningen lämnar flera nya förslag som bland annat innefattar masslagring av data i vissa situationer och som möjliggör inhämtning av elektronisk information i andra länder:

1) Nationell säkerhetslagring. Innebär att en generell och odifferentierad lagringsskyldighet avseende hela Sverige kan beslutas för en tvåårsperiod om det anses nödvändigt för att bekämpa ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt.

2) Geografiskt riktad lagring och utökad lagring. I syfte att bekämpa grov brottslighet föreslås riktade lagringsåtgärder beträffande kommuner där förekomst av grov brottslighet är högre än i andra. Vidare föreslås en möjlighet till utökad riktad lagring i förhållande till ett begränsat geografiskt område där grov brottslighet har förekommit och eller där det är sannolikt att sådan kan ske: en skyddsvärd plats, en person som dömts för grova brott eller teknik.

3) Exekutiv jurisdiktion, vilket innebär att svenska myndigheter ska kunna inhämta elektronisk information som är eller kan lagras utanför Sveriges gränser.

2.3 Behov av ett mer evidensbaserat förhållningssätt

Juridiska fakultetsnämnden finner som helhet att de förslag som lämnas avseende nationell säkerhetslagring, geografiskt riktad lagring samt exekutiv jurisdiktion kräver ytterligare genomarbetning och analys i flera avseenden.

Att införa nya former av lagringsskyldigheter varigenom individers privatliv kan kartläggas på ett ingående sätt, ställer lagstiftaren inför en komplicerad balansakt mellan flera betydelsefulla intressen, såsom effektivitet och integritet. Sådana åtgärder måste, som också understryks i utredningen, vara proportionerliga och strikt nödvändiga i ett demokratiskt samhälle. Dessa intressen är inte alltid oförenliga, men riskerna med massövervakning kan inte nog understrykas. Det finns inte heller något som styrker ett grundantagande att massövervakning leder till en effektiv brottsbekämpning.[4]

Det förekommer emellertid få hänvisningar i utredningen till litteratur och forskningsresultat avseendes effektiviteten med massövervakningsåtgärder, vilket gör det svårt att bilda sig en uppfattning om vilket material utöver gällande rätt som ligger till grund för de slutsatser som dras. Det saknas empiri i stor utsträckning, vilket troligen delvis kan förklaras av komplexiteten av att bedriva forskning när hela eller delar av forskningsunderlaget kan vara hemligstämplat. Oavsett hur det förhåller sig härmed finns få referenser till forskning på området och några forskningsrapporter har inte utförts på utredningens uppdrag. Problemet med detta är i första hand att det inte ger något fullödigt underlag för att avgöra på vilket sätt de åtgärder som föreslås verkligen är effektiva för att bekämpa hot mot nationell säkerhet eller grov brottslighet enligt förslaget, som kan motivera de betydande inskränkningar i fri- och rättigheter som de innebär.

Bristen på evidens innebär också att valet av lagstiftningsmodell inte får den underbyggnad som behövs. Det ska också påpekas att de nya lagringsåtgärderna reser komplexa frågor som skulle behöva belysas i ett multidisciplinärt perspektiv.[5]

---

[4] Se t.ex. Marx, Gary T., A Tack in the Shoe: Neutralizing and Resisting the New Surveillance, Journal of Social Issues Vol. 59, No 2, 2003, s. 369.
[5] Lyon, David, Surveillance Studies: An Overview, Polity Press, Cambridge, U.K. 2007, s. 18 f.

Det står klart att dansk lagstiftning varit en inspiration, men de komparativa jämförelserna är mycket kortfattade. Det framgår inte vilken metod som har använts för denna studie och inte heller varifrån uppgifterna kommer. Det förekommer ingen närmare redogörelse för de brister de olika modeller som beskrivs uppvisar eller kritiseras för. Avseende den belgiska lagstiftningen anges att denna för närvarande är föremål för en rättsprocess i den belgiska författningsdomstolen (*Cour constitutionelle*).[6] Vad som är mer förvånande är att det danska systemet, som utgör den huvudsakliga förebilden för förslagen om riktad lagring, beskrivs på ett så summariskt sätt. För att kunna göra en nyanserad bedömning av valet av lagstiftningsmodell i denna del, gäller det att också redovisa den kritik som har framförts mot den danska lagstiftningen, så att den svenska modellen kan utformas med beaktande av detta. Det är viktigt att undvika att göra om misstag och göra modellen mer träffsäker och rättssäker.

Det är således flera frågor som lämnas utan svar. I vilken utsträckning är datalagring och åtkomst till elektronisk information via olika leverantörer avgörande för att avvärja hot mot nationell säkerhet och uppklarandet av grova brott? Om underlaget är bristfälligt, av vilka andra skäl är det då strikt nödvändigt att utföra de omfattande massövervakningsåtgärder som föreslås? Vilka andra alternativ står till buds i form av andra mer riktade övervakningsåtgärder eller redan tillgängliga tvångsmedel? Vilka alternativa modeller till datalagringsskyldighet finns i andra länder, t.ex. den bevarandeskyldighet som införts i Österrike. Finns det andra åtgärder än datalagring som kan vara ett alternativ för Sverige?[7] Enligt Juridiska fakultetsnämnden ges inga tydliga svar på dessa frågor som gör det möjligt att från ett utomstående perspektiv göra en bedömning i vilken utsträckning de åtgärder som föreslås är proportionerliga.

Behov av undantag

Utredningen är angelägen om att lämna ett förslag som följer EU-domstolens praxis på området. Det är bra, men Juridiska fakultetsnämnden finner att det saknas mer utvecklade principiella ställningstaganden som är hänförliga till riskerna med en omfattande masslagring för såväl rättssystemet som samhället i stort. Detta gäller t.ex. de problem som föreligger vid lagring som kan avslöja mycket känsliga uppgifter och där det till och med kan vara förenat med allvarlig fara för individers liv och hälsa om dessa uppgifter lagras. Det handlar t.ex. om hjälplinjer för psykologiska och sociala kriser, t.ex. BRIS och kvinnofridslinjen, kommunikation mellan t.ex. läkare, psykologer och deras patienter m.m. Den s.k. Vaastamo-läckan i Finland 2020 är ett varnande exempel på vilka risker som finns.[8] EU-domstolen har tagit upp denna problematik vid upprepade tillfällen i sin praxis avseende datalagring. Denna mycket viktiga problematik analyseras emellertid inte närmare i betänkandet. Är det möjligt att göra undantag och i så fall vad kan och bör göras?

---

[6] SOU 2023:22, s. 253.

[7] Birrer, Alena, He, Danya, Just, Natascha, The state is watching you – A cross-national comparison of data retention in Europe, Telecommunications Policy 47, 2023, s. 5. Birrer et al. Redogör i denna artikel för att Österrike har övergivit datalagringsregimen till förmån för ”data preservation”, vilket vi översätter som en bevarandeskyldighet. Författarna anger att den nya modellen emellertid är behäftad med liknande problem som den för datalagring. Icke desto mindre hade det varit betydelsefullt om utredningen hade fått i uppdrag att belysa alternativ till datalagring.

[8] Lindberg, Milli, *Nästan 32 000 patientjournaler från Vastaamo-läckan publicerades igen på Tor-nätverket*, Svenska Yle 2021-01-27.
Se även Dataombudets byrå (Finland), pressmeddelande av den 27 december 2021, Påföljdsavgifter för dataskyddsöverträdelser åt psykoterapicentret Vastaamo (publicerad på finska 16 december 2021), https://tietosuoja.fi/sv/-/pafoljdsavgift-for-dataskyddsovertradelser-at-psykoterapicentret-vastaamo.

Risken för fel och missbruk

Hur risken för fel och missbruk ska avvärjas och hanteras bör noga penetreras. Sådana faktorer är avgörande för att bedöma om den data som lagras kan läggas till grund för t.ex. beslut om olika polisiära åtgärder eller om den är tjänlig som bevis i brottmål. Ett intressant exempel på att det kan gå snett är den danska teledata-skandalen 2019. Felet berodde på ett systemfel i polisens datasystem rörande platsdata. Inledningsvis upptäcktes att inte alla telefoner som var kopplade till telemasterna visades i programmet. Därefter stod det klart att det överhuvudtaget inte var möjligt att lita på att de positioner som visades i programmet stämde. Dessa brister ledde till att cirka 10 000 brottmål mellan 2012 och 2019 måste undersökas om huruvida en omprövning kunde vara nödvändig eller ej. Dessutom innebar detta att flera brottsmisstänkta försattes på fri fot. Under tiden infördes också ett tillfälligt förbud att använda mobildata som bevis i brottmål.[9]

I det aktuella systemet med datalagring finns vidare en inneboende risk för missbruk, då den kan öppna upp för en omfattande kartläggning av individers förehavanden. EU-domstolen har beskrivit detta avseende trafik- och lokaliseringsuppgifter enligt följande i fallet SpaceNet:

> ”…trafik- och lokaliseringsuppgifter kan avslöja information om ett stort antal aspekter av de berörda personernas privatliv, inbegripet känslig information, såsom sexuell läggning, politisk åskådning, religiös, filosofisk eller annan övertygelse, samhällsåskådning samt hälsotillstånd, samtidigt som sådana uppgifter omfattas av ett särskilt skydd enligt unionsrätten. Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. Närmare bestämt gör dessa uppgifter det möjligt att upprätta en profil för de berörda personerna, och denna information är lika känslig ur integritetssynpunkt som själva innehållet i kommunikationerna.”[10]

Risken för missbruk gäller inte endast staten utan även leverantörerna. I EU-domstolens praxis lyfts särskilt fram att:

> ”Med hänsyn till den stora mängd trafik- och lokaliseringsuppgifter som kan bli föremål för fortlöpande lagring genom en generell och odifferentierad lagringsåtgärd och till att den information som dessa uppgifter kan innehålla, är känslig, medför den omständigheten att leverantörer av elektroniska kommunikationstjänster lagrar dessa uppgifter i sig en risk för missbruk och obehörig åtkomst”.[11]

---

[9] Fridh Kleberg, Carl, *Dataskandal skakar danska rättsväsendet – nu släpps misstänkta fria*, SVT 22 augusti 2019, https://www.svt.se/nyheter/utrikes/dataskandal-skakar-danska-rattsvasendet-nu-slapps-misstankta-fria (hämtad oktober 2023). En undersökning av den danska Rikspolisen hantering av historiska teledata gjordes härefter av Deloitte på uppdrag av Rigspolitiet, se Deloitte, *Undersøgelse af Rigspolitiets håndtering af historiske teledata*, 1 oktober 2019, bilag 3.

[10] De förenade målen C-793/19 och C-794/19, *SpaceNet och Telekom Deutschland*, dom (stor kammare) av den 20 september 2022, p. 61.

[11] Se t.ex. mål C-140/20, *Commissioner of An Garda Síochána*, dom (stor kammare) av den 5 april 2022, p. 46 och de förenade målen C-793/19 och C-794/19, *SpaceNet och Telekom Deutschland*, dom (stor kammare) av den 20 september 2022, p. 62.

Risker som kan vara hänförliga till den outsourcing av övervakningsuppgifter till privata företag som den aktuella ordningen innebär och hur det ska hanteras är inte föremål för någon självständig analys.[12] Detta kommer att utvecklas ytterligare nedan avseende risken för infiltration i dessa bolag. Leverantörerna av elektronisk kommunikation, vilket i synnerhet gäller Noik, är vidare ofta inte svenska företag, vilket kan innebära problem med att få tillgång till lagrade uppgifter om elektronisk kommunikation om detta inte regleras i internationell rätt. Det bör vidare analyseras om denna outsourcing kan få konsekvenser för den nationella säkerheten avseende nationell säkerhetlagring.

Sammanfattningsvis kan sägas att det behövs mer empiri beträffande effektiviteten i de åtgärder som föreslås och en utredning som möjliggör en diskussion om alternativa åtgärder.

3. Kommentarer till utredningens förslag

3.1 Nationell säkerhetslagring

Nationell säkerhetslagring innebär enligt förslaget, att en generell och odifferentierad lagringsskyldighet avseende hela Sverige kan beslutas för en tvåårsperiod om det anses nödvändigt för att bekämpa ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt.

Juridiska fakultetsnämnden ifrågasätter inte att nationell säkerhetslagring i vissa fall kan vara en strikt nödvändig åtgärd för att avvärja och bekämpa hot mot den nationella säkerheten om det omgärdas av tillräckliga rättssäkerhetsgarantier.

Det är möjligt att lagring av kommunikationsdata rörande individer *en masse* bör tillåtas trots den integritetskränkning detta innebär, men då måste riskerna för fel och missbruk beaktas.[13] Härvid är det av avgörande betydelse om en sådan åtgärd verkligen är effektiv, i synnerhet som den är tänkt att omfatta hela Sverige. Följaktligen är det av betydelse hur dessa enorma datamängder är tänkta att hanteras, vilket ställer höga krav på förfarandet vid användningen av dessa data inte bara från rättsliga utgångspunkter utan även från ett tekniskt och organisatoriskt perspektiv.[14]

Någon forskning eller statistik som backar upp antagandet om den nationella säkerhetslagringens påstådda effektivitet för att bekämpa hot mot den nationella säkerheten eller tydliga exempel på i vilka situationer som datalagring är effektivt och nödvändigt för att bekämpa sådana redogörs inte närmare för i betänkandet. Generella hänvisningar görs i författningskommentaren till terrorism, allvarliga och skadliga cyberangrepp, förhöjd terrorhotnivå i landet, hot om väpnat angrepp och därmed jämförliga situationer.[15]

Åtgärdernas effektivitet bör vidare ses i ljuset av att t.ex. terrorister och spioner har möjligheter att ”gå under radarn” t.ex. genom krypterade telefoner. Sådana grupperingar tenderar också att utveckla

[12] Detta synes följa ett internationellt mönster med vissa undantag såsom Schweiz, vilket kan vara värt att undersöka närmare, se Birrer et al. 2023, s. 7.
[13] Sorell, Tom, *Privacy, bulk collection and “operational utility* i Miller, Seumas, Regan, Mitt & Walsh, Patrick F., National Security Intelligence and Ethics, Routledge, New York 2022, s. 141-155.
[14] Se t.ex. Gordon, Matthew, *Big data: It´s Not the Size That Matters*, Journal of National Security Law and Policy, vol. 7, nr. 2, 2014, s. 311-324.
[15] SOU 2023:22, s. 515 f.

och använda teknologi för att förhindra eller försvåra övervakning.[16] Det finns säkerligen andra data rörande elektronisk kommunikation som är viktiga för att bekämpa sådana hot, men frågan är i vilken mån sådan insamling av data är avgörande för att avvärja hotet eller på annat sätt är nödvändigt för detta ändamål eller om det finns likvärdiga alternativa åtgärder.

En annan risk som bör bli föremål för vidare analys tar sikte på tolkningen av hot mot nationell säkerhet, så att denna inte blir för vidsträckt och bidrar till s.k. *surveillance creep*, d.v.s. att det sker en målförskjutning och expansion av övervakningsåtgärderna.[17] Utredningen anser inte att några kriterier ska föreskrivas för detta, vilket i och för sig är förståeligt, då det är svårt att förutse vilka situationer som kan uppstå i framtiden.[18] Ett gediget förfarande för sådant beslutsfattande är centralt, men det förtar inte det faktum att det finns en risk för att lokutionen ”allvarligt hot mot den nationella säkerheten som är verkligt och aktuellt eller förutsebart” får en alltför vid tolkning, vilket kan leda till felaktiga beslut och/eller innebära ett missbruk av nationell säkerhetslagring. Mer konkret kan det innebära att den nationella säkerhetslagringen de facto permanentas. Ett riskbaserat förhållningssätt ter sig nödvändigt, vilket kan realiseras genom ett noga utformat förfarande.

Förfarandet

Helt centralt för bedömningen av hot mot nationell säkerhet är som ovan nämndes ett gediget förfarande. Enligt förslaget ska Säkerhetspolisen (Säpo) göra bedömningen avseende det nationella säkerhetshotet under kontroll av ett nytt särskilt beslutsorgan inom Säkerhets- och integritetsskyddsnämnden, den s.k. Datalagringsdelegationen. Ett offentligt ombud ska enligt förslaget inrättas som ska bevaka enskildas intressen och denna aktör ska också kunna överklaga Säpos beslut.[19]

Förfarandet liknar i viss mån den modell som gäller för signalspaning, vilket regleras enligt lag (2009:966) om Försvarsunderrättelsedomstol. Frågor om signalspaning prövas av en specialdomstol, Försvarsunderrättelsedomstolen och i processen deltar ett ombud med uppdrag att ta tillvara enskildas intressen, integritetsskyddsombudet. Detta får anses vara en lämplig och beprövad modell med tämligen hög grad av legitimitet.[20]

I det aktuella förslaget är emellertid samtliga aktörer i förfarandet förvaltningsmyndigheter. Detta är ett inslag som i viss mån framstår som hänförligt till en annan tid, då domstolsprövning många gånger inte ansågs nödvändigt vid beslut med stora konsekvenser för enskildas fri- och rättigheter.

---

[16] Se Marx 2003 s. 372. Marx framhåller (s. 372) att: “Humans are wonderfully inventive at finding ways to beat control systems and to avoid observation. Most surveillance systems have inherent contradictions, ambiguities, gaps, blind spots and limitations, whether structural or cultural, and, if they do not, they are likely to be connected to systems that do.”

[17] Marx, Gary T., *Surveillance Studies*, International Encyclopedia of the Social & Behavioral Sciences, andra upplagan, s. 738.

[18] SOU 2023:22, s. 186 f.

[19] Ibid., s. 196 ff.

[20] Hansén, Dan, *Assessing intelligence oversight: the case of Sweden*, Intelligence and National Security 2023, DOI: 10.1080/02684527.2023.2222534; Det ska också kommenteras att det förekommit en debatt enligt vilken det ifrågasattes om Försvarsunderrättelsedomstolen utgör en domstol enligt det europarättsliga domstolsbegreppet, se Otter Johansen, Tormod & Wejedal, Sebastian, *Mot ett funktionellt domstolsbegrepp – ett bidrag med anledning av den s.k. Försvarsunderrättelsedomstolen (del II av II)*, Svensk Juristtidning 2016, s. 191-232.

Juridiska fakultetsnämnden anser att förslaget är i behov av förstärkning i denna del, i synnerhet som det är fråga om lagstiftning som rör nationell säkerhetslagring som omfattar hela befolkningen. Det framstår därför som mer lämpligt att beslutet prövas antingen av Högsta domstolen eller av Försvarsunderrättelsedomstolen. Högsta domstolen har den kompetens som krävs och dömer i frågor om brott mot Sveriges säkerhet. Att HD fattar beslut om nationell säkerhetslagring har också ett viktigt värde för att markera allvaret i situationen.

Ett annat alternativ är att utöka Försvarsunderrättelsedomstolens mandat, där det redan finns kompetens rörande nationell säkerhet, en etablerad organisation och befintliga arbetsrutiner. Det framstår vidare inte som tillfredsställande att frågan om nationell säkerhetslagring endast bedöms på myndighetsnivå. Det innebär i praktiken ”ett monopol” för regeringsmakten beträffande tolkningen av vad som ska avses med ett ”allvarligt hot mot den nationella säkerheten som är verkligt och aktuellt eller förutsebart.”[21]

En viktig synpunkt är vidare att det offentliga ombudet för att kunna utföra sitt uppdrag att bevaka enskilda intressen, bör ha en så oberoende ställning i förhållande till beslutsmyndigheten som möjligt. Juridiska fakultetsnämnden motsätter sig därför med bestämdhet förslaget i den del som säger att beslutsmyndigheten ska besluta om ombudets ersättning.[22] Beslut härom bör istället fattas av domstolen.

3.2 Lagring för att bekämpa grov brottslighet som inte utgör ett hot mot den nationella säkerheten

3.2.1 Geografisk riktad lagring

Juridiska fakultetsnämnden utesluter inte att geografiskt riktad lagring kan vara strikt nödvändigt i vissa situationer, men finner inte att utredningen ger tillräckliga skäl för att konstruktionen av dess förslag i denna del uppfyller de krav på träffsäkerhet och effektivitet som torde krävas för att åtgärden ska anses proportionerlig.

Utredningen presenterar inget underlag som ger en möjlighet att göra en objektiv bedömning av på vilket sätt en geografiskt riktad lagring som omfattar stora geografiska områden och en stor del av Sveriges befolkning är strikt nödvändig och effektiv för att utgöra ett legitimt avsteg från grundläggande rättssäkerhetsprinciper och skyddet för den personliga integriteten och särskilt rätten till skydd för personuppgifter. Grunderna för detta framstår emellertid som alltför vaga för att Juridiska fakultetsnämnden ska kunna tillstyrka förslaget. Det föreligger vidare omständigheter, vilka diskuteras ovan och som vidare redogörs för nedan, som talar emot effektiviteten med förslaget om en geografiskt riktad lagring och som närmare måste analyseras.

Geografiska områden och ”criminal hot spots”

Att geografiska faktorer kan vara av stor betydelse för ett effektivt polisarbete, såsom geografisk profilering av en misstänkt brottsling, framstår som okontroversiellt. Detta framstår som motiverat

[21] Flyghed, Janne, *Utrikespolitiken och rätten. Exemplet spioneri och sabotage i Sverige under andra världskriget* i Estrada, Felipe et al., I rättsstatens sprickor – En vänbok till Janne Flyghed, Kriminologiska institutionen, Stockholms universitet, Stockholm 2021, s. 42.
[22] SOU 2023:22, s. 196.

i flera situationer, t.ex. för att följa geografiska positioner för kreditkortstransaktioner för att söka avgöra var en person, misstänkt för grov brottslighet, befinner sig eller har sin hemvist.[23]

Utredningen söker finna en lösning som är tillräckligt avgränsad för att den ska kunna uppfylla EU-domstolens praxis på området och som har sin förebild i dansk lagstiftning. Frågan är emellertid om den avgränsning som görs är tillfyllest. Underlaget för beslut om geografiskt riktad lagring ska bygga på ”objektiva kriterier”, vilket likt det danska systemet innebär att det ska baseras på den officiella statistiken över anmälda brott. När det gäller det geografiska området, frångår emellertid utredningen ordningen i den danska lagstiftningen där 3 gånger 3 km utgör ett område för geografiskt riktad lagring. Detta anses inte möjligt för svenskt vidkommande mot bakgrund av hur brottsstatistiken redovisas i Sverige. Utredningen landar i att kommuner i vilka det enligt den officiella statistiken förekommer ett genomsnitt av anmälda brott delat med befolkningsmängden under en treårsperiod föregående lagringen, ska vara de områden inom vilka en geografiskt riktad lagring kan ske.[24]

Enligt en ögonblicksbild som redovisas i betänkandet skulle detta gränsvärde motsvara 92,1 anmälda brott per 1000 invånare räknat utifrån brottsanmälningar per kommun för åren 2020–2022. Detta skulle enligt den aktuella beräkningen innefatta en riktad lagring i 132 av Sveriges 290 kommuner och cirka 7,3 av Sverige 10,4 miljoner invånare.[25]

I betänkandet diskuteras möjligheten att avgränsningen av det geografiska området skulle kunna avgränsas bättre om Brottsförebyggande rådet (Brå), som tar fram denna statistik, tydligare skulle kunna ringa in den grova brottsligheten till mindre områden. Utredningen gör emellertid bedömningen att fördelarna med detta inte väger upp för det merarbete som detta skulle innebära för Brå.[26]

Juridiska fakultetsnämnden ställer sig tveksam till den föreslagna ordningen av flera skäl. En första fråga är hur effektivt det är att förlita sig på ett system med geografiskt riktad lagring utifrån vissa givna gränsvärden. I det särskilda yttrandet problematiseras till exempel kring problem med tröskeleffekter[27] - en kritik som Juridiska fakultetsnämnden delar. Ett annat problem kan vara att det sker en anpassning till detta bland grovt kriminella personer och nätverk. Istället för att verka från t.ex. Stockholm är det istället möjligt att bosätta sig i eller verka från Nykvarn eller Värmdö med bibehållen närhet till huvudstaden utan att riskera att omfattas av en åtgärd med geografisk riktad lagring. Kriminella personer i Göteborg som enligt förslaget skulle vara föremål för geografiskt riktad lagring kan istället flytta eller förlägga den brottsliga verksamheten till den närliggande kommunen Mölndal. För verksamhet belägen i Sundsvall, som skulle överskrida gränsvärdet, skulle Timrå kommun, som hamnar under gränsvärdet, kunna utgöra ett alternativ för kriminella grupperingar som vill undgå sådan lagring. Sådana anpassningar av den kriminella verksamheten i kombination med användning av alternativa krypterade kommunikationstjänster, skulle delvis kunna omintetgöra effektiviteten i det aktuella förslaget.

---

[23] Clark, Robert M., *Intelligence Analysis: A Target-Centric Approach*, 6e uppl. SAGE, U.K., 2020, s. 393 f.
[24] SOU 2023:21, s. 252 f.
[25] Ibid., s. 261.
[26] Ibid. s. 259.
[27] Ibid. s. 578.

Vidare finns det aktuella exempel på att grovt kriminella personer kan leda organiserad brottslighet i Sverige utan att befinna sig i Sverige. Ett aktuellt exempel är den så kallade ”Kurdiska räven”, ledare för den kriminella organisationen Foxtrot, som sedan flera år varit bosatt i Turkiet. Nyligen har denne enligt medias rapportering och uppenbarligen från en plats utanför Sveriges och EU:s gränser, uttalat sig om att Strängnäs skulle vara ”hans område”.[28]

Alternativa krypterade kommunikationstjänster

Bilden av att det finns problem med att använda sig av geografisk positionering som utgångspunkt förstärks t.ex. av polisens rapport avseende lärdomarna från Encrochat från 2021.[29] Encrochat var en kommunikationstjänst som möjliggjorde krypterad kommunikation och som i stor utsträckning användes av kriminella organisationer i deras verksamhet. År 2020 lyckades fransk polis och Europol med att dekryptera tjänsten, vilket innebar att polismyndigheter i flera länder däribland Sverige kunde följa brottsplanering i realtid, vilket ledde till ett stort antal uppklarade brott och fällande domar.[30]

Encrochat-erfarenheterna visar på flera faktorer som innebär att krav på datalagring av vanliga kommunikationstjänster kanske inte är den guldgruva av underrättelseinformation beträffande grov brottslighet som skulle kunna innebära att masslagring av sådana data skulle kunna vara strikt nödvändig.[31]

För det första står det klart att grovt kriminella verkar välja krypterad kommunikation för att kommunicera med varandra i sin kriminella verksamhet snarare än via gängse kommunikationstjänster, vilket inte torde vara ägnat att förvåna. Encrochat och SkyECC var krypterade kommunikationstjänster som avvecklats på grund av gediget polisarbete. Icke desto mindre fortsätter enligt polisen kommunikationen mellan grova kriminella på andra krypterade plattformar.[32] Det ska tilläggas att det också har förekommit exempel där brottsbekämpande myndigheter har infiltrerat organiserad brottslighet genom att skapa en egen krypterad plattform, såsom FBI:s plattform Anom inom *Operation Trojan Shield/Greenlight*, i vilket Sverige deltog.[33]

---

[28] Pfriem, Johan, Asplund, Fanny, *Kurdiska räven Rawa Majids hotfulla meddelande: ”Ingen rör Strängnäs”*, SVT Nyheter, uppdaterad 5 oktober 2023, publicerad 7 april 2023, se https://www.svt.se/nyheter/lokalt/sormland/kriminella-ledaren-kurdiska-ravens-hotfulla-meddelande-ingen-ror-strangnas

[29] Polisen, NOA, strategisk rapport, dnr A193.902/2021, *Lärdomar av Encrochat – Analysprojekt Robinson*.

[30] Se Europol:s hemsida, News 27 June 2023, *Dismantling encrypted criminal EncroChat communications leads to over 6500 arrests and close to EUR 900 million seized –Judiciary and law enforcement present first overview of results*, se https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized (hämtad oktober 2023).

[31] Ett annat exempel är erfarenheterna kring kommunikationstjänsten Sky ECC, som dekrypterades av holländsk polis. Värt att påminna om är även tjänsten Anom, som utvecklades och drevs av amerikanska FBI och som lurade kriminella att använda tjänsten. Se t.ex. Eklund Henning, *Hundratals gripna efter att FBI skapat falsk krypteringsapp*, NyTeknik 8 juni 2021.

[32] Polisen, NOA, strategisk rapport, dnr A193.902/2021, *Lärdomar av Encrochat – Analysprojekt Robinson*, s. 31.

[33] Se t.ex. Europols hemsida, *800 criminals arrested in biggest ever law enforcement operation against encrypted communication*, 8 juni 2021, https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication (hämtad i oktober 2023).

För det andra visar polisens rapport på en inte obetydlig geografisk rörlighet bland de kriminella nätverken. Av det aktuella materialet befann sig 40 procent i Sverige, av vilka 40 procent i Stockholm och 15 procent var utomlands (främst Nederländerna och Spanien). Beträffande den resterande delen om 45 procent saknades information om geografisk placering. Enligt rapporten föreligger interregionala nätverk som präglas av samarbete för att uppnå maximal ekonomisk vinning, snarare än konkurrens.[34]

Objektiva kriterier

När det gäller frågan om objektiva kriterier kan officiell statistik vara lämpligt att använda. Utredningen lyfter emellertid fram att det skulle kunna vara möjligt att avgränsa den geografiskt riktade lagringen ytterligare och därmed öka träffsäkerheten om brottsstatistiken redovisades på ett annat sätt. Något förslag om att Brå skulle ges ett nytt uppdrag lämnas emellertid inte med hänvisning till argumentet att utredningen inte bedömer att ”fördelarna med ett sådant underlag är tillräckliga för att väga upp det merarbetet som uppdraget skulle innebära”. Detta argument framstår inte som särskilt övertygande, när det handlar om ett alternativ som gör det möjligt att minska kretsen av individer som omfattas, varav den stora majoriteten inte har några kriminella förehavanden, att bli föremål för geografiskt riktad lagring.

Riskerna för infiltration m.m.

Avslutningsvis ska en annan aspekt på datalagringens effektivitet diskuteras. Det föreligger, som polisen lyfter fram i sin Encrochat-rapport ”ett högt säkerhetstänk” bland aktörerna i materialet, vilket även ger sig till känna i hur den kriminella verksamheten organiseras, bland annat genom infiltration i olika legala verksamheter såsom banker, myndigheter och företag. Sistnämnda ger anledning att fråga sig i vilken utsträckning infiltration kan förekomma bland de tjänsteleverantörer som utför datalagringen för statens räkning. Detta är en faktor som inte kan bortses ifrån när det gäller att bedöma masslagringens effektivitet. Kan data som levereras vara förvanskad eller finns det uppgifter som kan vara förstörda på grund av eventuell infiltration? Möjligheten att det kan förekomma infiltration är inte något som ensamt skulle innebära att masslagring enligt förslaget skulle vara uteslutet, men är en fråga som har stor betydelse för allmänhetens förtroende för åtgärden samt de risker som detta kan innebära för persondataskyddet och därför kräver ytterligare utredning och analys.

3.2.2 Utökad riktad lagring

Förslaget om utökad riktad lagring företer flera likheter med den geografiskt riktade lagring när det gäller grundläggande brister. Utökad riktad lagring framstår emellertid som mer avgränsad och precis. Det finns emellertid anledning att fråga sig i vilken utsträckning en sådan åtgärd om den genomförs kommer att vara effektiv. När det gäller riktad lagring vid skyddsvärda platser såsom bussterminaler och flygplatser är frågan om detta kommer att vara verksamt. Om grovt kriminella väljer alternativa kommunikationstjänster finns det risk att de inte fångas upp. Istället är det vanliga, laglydiga löntagare som åker till och från jobbet som i praktiken omfattas av lagringen.

3.2.3 Förfarandena kring den riktade lagringen

Utredningen föreslår att beslut som avser riktad lagring ska fattas av olika myndigheter.

---

[34] Polisen, NOA, strategisk rapport, dnr A193.902/2021, *Lärdomar av Encrochat – Analysprojekt Robinson*, s. 8.

Beslut om vilka kommuner som ska omfattas av geografiskt riktad lagring ska fattas av Post- och Telestyrelsen (PTS) emedan beslut om utökad riktad lagring ska kunna fattas av Polismyndigheten, Säkerhetspolisen och Tullverket. Denna fördelning framstår i viss mån som rationell, men kan vara krånglig i praktiken, då främst för leverantörerna.

Det framstår vidare inte som tillfredsställande att de riktade lagringsåtgärderna inte om-gärdas av samma skyddsmekanismer som vid nationell säkerhetslagring och signalspaning.

Juridiska fakultetsnämnden vill framhålla att det mest lämpliga i sammanhanget är att geografiskt riktad och utökad riktad lagring, om de införs, inte kan ske utan beslut av en oberoende och opartisk domstol. Detta grundar sig på flera skäl. För det första är det fråga om starkt rättighetsinskränkande åtgärder, vilket motiverar att myndigheten får lägga fram sin begäran inför en domstol och inte en förvaltningsmyndighet. Detta bör ske i de allmänna domstolarna, som beslutar om tvångsåtgärder och dömer i fall rörande grov brottslighet. För det andra kan domstolen få en överblick över de åtgärder som används i övrigt. Detta gäller t.ex. utökad riktad lagring avseende en person. Är det så att samma person är föremål för flera åtgärder samtidigt, t.ex. utökad riktad lagring och hemlig dataavläsning, är det möjligt för domaren att få en tydlig överblick över dessa. För det tredje har de allmänna domstolarna en betydande kompetens avseende straffrättsliga och straffprocessuella frågor, såsom hemlig dataavläsning. De borde därför vara bäst skaffade att fatta beslut om datalagringsåtgärder som sker för att bekämpa grov brottslighet.

Beslut om geografiskt riktad lagring ska ske en gång per år med utgångspunkt i den officiella statistiken. I praktiken innebär det att kommuner som har högre andel grova brott i jämförelse med andra kommuner, konstant kommer att vara föremål för på varandra följande massövervakningsåtgärder. Det är också otillfredsställande att det inte föreslås åtgärder för de fall då övervakningsåtgärden inte längre är strikt nödvändig, t.ex. om en lyckad polisoperation, såsom *Operation Trojan Horse*, medför att brottsanmälningarna inom en viss kom-mun, kraftigt minskar på kort tid. En liknande situation kan gälla grupper av personer som bor nära en skyddsvärd plats och som troligen år från år kommer att vara föremål för denna riktade lagring eftersom flygplatser och tågstationer normalt inte flyttas.

Det framstår också som svårt att förstå varför endast personer som tidigare varit dömda för grova brott eller personer som tidigare varit föremål för hemliga tvångsåtgärder ska kunna vara föremål för utökad riktad lagring. Det verkar föga träffsäkert och medför en risk för stigmatisering. Det blir vidare svårt att utföra en sådan riktad åtgärd angående personer som är misstänkta för grov brottslighet, vilket kan vara angeläget.

Vid en sammantagen bedömning framstår förslaget i själva verket till stor del inte som riktade åtgärder i egentlig bemärkelse och kan därmed inte anses proportionerliga.

3.3 Angående vissa frågor om exekutiv jurisdiktion

3.3.1 Sammanfattning

Utredningens uppdrag vad gäller exekutiv jurisdiktion bestod, enligt direktiven, i att “analysera de folkrättsliga frågorna om exekutiv jurisdiktion i förhållande till elektroniska uppgifter utanför Sverige, och i denna analys även göra en jämförelse med rättsläget i andra relevanta länder.” Utredningen föreslår i denna del att “brottsbekämpande myndigheter genom straffprocessuella tvångsmedel [får] inhämta elektronisk information som är lagrad utanför Sverige“ (1 §) under förutsättning att det kan ske “utan bistånd“ (§ 2) och att det inte innebär “mer än ett obetydligt intrång i en annan stats suveränitet“ och inte “orsaka[r] någon skada på det in-formationssystem som tvångsmedlet avser.“

3.3.2 De folkrättsliga resonemangen i stort

Det material som används för den folkrättsliga analysen är synnerligen magert. I doktrinen refereras till två svenska läroböcker på grundkursnivå. Vidare citeras material från Europarådet och EU vad gäller andra väststaters praxis, men ingen praxis från andra länder, ej heller referenser till andra regionala eller till globala organisationer.

Frågan om vad som utgör ett folkrättsvidrigt intrång i suveräniteten med avseende på olika cyberåtgärder har varit den kanske mest omdebatterade frågan i de långdragna FN-diskussionerna sedan 1998 om nationell säkerhet i ”cyberrymden”. Ett antal stater, däribland Sverige, har avgivit positionspapper där man angett sina synpunkter på denna och andra frågor. Förutom Europarådets Budapestkonvention finns åtminstone tre regionala konventioner och för närvarande pågår förhandlingar om en global cyberbrottskonvention i FN. Det finns också idag en ganska omfattande internationell juridisk litteratur om dessa frågor. Inget av detta har dock avspeglats i utredningen.

Bristerna i underlaget påverkar på många sätt utredningens resonemang.

För det första har man en ovanlig uppfattning om hur den territoriella suveräniteten ska tillämpas för nu aktuella frågor. I utredningen hänvisas till det vägledande s k Lotusmålet från 1927: ”Verkställigheten av nationella lagar och domar (t.ex. gripande eller beslag) kan … äga rum endast inom det egna territoriet” (s 129; se även s 133 f samt s 433). Sedan konstaterar utredningen att ”[i] den digitala världen ser förhållandena annorlunda ut” (s 434). Därefter diskuteras innehållet i sedvanerätten vad gäller elektronisk information som lagras utanför den egna statens territorium, och man konstaterar att “det inte finns någon internationell sedvanerätt på nu aktuellt område“ (s 467). Detta är en uppfattning som delas av den brittiska regeringen och av USA:s försvarsdepartement men av i stort sett ingen annan regering, inte ens den svenska. Den förhärskande uppfattningen är istället att intill dess att sedvanerätten förändrats så gäller territoriellt suveränitet också i “cyberrymden“, medan det är oklart exakt *hur* den gäller.
För det andra är urvalet av länder helt otillfredsställande (ss 451 ff). När det i en utredning görs en ”utblick” görs det vanligen för att underlätta för lagstiftaren att bedöma hur utredningens förslag förhåller sig till lagstiftningen i länder som vi vanligen jämför oss med och av vilka vi kan lära. Om avsikten är att med hjälp av statspraxis bedöma sedvanerättens inställning måste urvalet emellertid se helt annorlunda ut, och då kan man inte inskränka sig till vänligt inställda stater i vårt närområde. Utredningen borde ha tittat på länder som är viktiga för rättsutvecklingen samt på länder som kan vara relevanta för den verksamhet det är fråga om, dvs länder där det kan tänkas finnas information som svenska brottsbekämpande myndigheter är intresserade av samt länder

som kan tänkas vara intresserade av information som finns lagrad i Sverige. Vad gäller direktåtkomst till elektronisk information har ett antal – men långt ifrån alla -- väststater en attityd som liknar den som utredningen föreslår. Det kan därför antas att flera av de stater där relevant information eller dokument finns lagrad (t ex Danmark) skulle godta agerande enligt utredningens förslag. Med tanke på amerikanska molnleverantörers dominans idag hade det emellertid varit särskilt relevant att undersöka de amerikanska attityderna avseende direkt åtkomst, vilket inte görs. Vidare måste länder som Kina, Indien, Ryssland och Brasilien beaktas, både därför att de är viktiga vad gäller skapandet av sedvanerätt och därför att Kina är en stor aktör inom t ex plattforms- och mjukvaruindustrin.

För det tredje används traktater på ett helt oreflekterat sätt som bevis på sedvanerätt, när det lika gärna kan vara det omvända, dvs att en grupp stater har sett det som önskvärt att komma överens om vissa regler sinsemellan just därför att de *inte* gäller sedvanerättsligt. När utredningen går igenom avtal och praxis från EU och Europarådet samt från ett litet urval stater konstaterarar man att ett antal länder idag verkar villiga att acceptera att andra länder bereder sig tillgång till information som finns lagrad i det egna landet, men det gäller inom en begränsad krets av ganska likartade länder.

Man borde också ha studerat rättsbildningsprocessen i Europarådet och EU genom ett sådant analytiskt raster. Åtgärder som inte ens statsparterna till Budapestkonventionen kan acceptera sinsemellan kan knappast anses godtagna i ett globalt perspektiv. I betänkandet berättas att den s k Molnbevisgruppen i Europarådet år 2016 föreslog att staterna skulle överväga att ge sig rätt till gränsöverskridande direktåtkomst till uppgifter utan samtycke från territorialstaten, under förutsättning att de brottsutredande myndigheterna på laglig väg fått fram inloggningsuppgifter till en molntjänst, dvs det som utredningen föreslår. Molnbevisgruppens mening var att en sådan bestämmelse skulle kunna inflyta i det som skulle bli det andra tilläggsprotokollet till Budapestkonventionen. Så skedde emellertid inte. Detta faktum skulle kunna tolkas så att parterna till konventionen inte var beredda att acceptera just det som utredningen nu föreslår. Huruvida den hypotesen stämmer kan bara utrönas efter studier av förhandlingsdokumentationen (eller kanske av en intervju med den svenska förhandlaren). Någon reflektion om den saken finns inte i betänkandet.

För det fjärde behandlas exempel på åtkomst till elektronisk information i statspraxis och rättspraxis utan urskiljning, trots att de utgör olika slag av utövande av jurisdiktion. När utredningen hävdar att det finns en ökad acceptans för åtkomst till elektronisk information i främmande länder åberopas ett stort antal exempel som handlar om åtkomst genom ombud, dvs tjänsteleverantör (molntjänster, Internettjänster, etc). Detta gäller t ex artikel 18 i Budapestkonventionen och dess andra tilläggsprotokoll liksom flera exempel på statspraxis, inklusive den åberopade norska Høyesterettsdomen från 2019 (se bl a ss 441-42, 444, 457, 467). I alla dessa fall har det inte varit fråga om att polisen tagit sig direkt exekutiv jurisdiktion på IT-system i en annan stat utan om att man har beordrat en tjänsteleverantör att ta fram de eftersökta dokumenten. Därvidlag har man baserat sig på jurisdiktion över tjänsteleverantören och inte över dokumenten. Det finns anledning att diskutera om sådan exekution genom ombud ska behandlas annorlunda än direkt exekution, men det är i vart fall så dessa domstolar och regeringar (i vart fall i stort) har motiverat sina ställningstaganden. Inte heller artikel 32(b) i Budapestkonventionen kan åberopas som bevis på ”användande av inloggningsuppgifter för att bereda sig tillgång till uppgifter på ett användarkonto på en internettjänst inte utgör en kränkning av den andra statens

suveränitet", eftersom det som avses i detta författningsrum inte kan anses utgöra dataintrång. F ö anser flera stater, bland dem Ryssland, att även artikel 32(b) går alltför långt.

Det kan inte uteslutas att en grundlig analys av gällande sedvanerätt skulle ge samma resultat som utredningen gjort. Materialet i utredningen ger dock inte underlag för en sådan slutsats, och Juridiska fakultetsnämnden betvivlar för övrigt att det är den riktiga.

3.3.3 Förslagen

Här ska förslagen i sig diskuteras.

Intrång

Med förbehåll för det som ovan anförts lämnas följande synpunkter med utgångspunkt i utredningens inriktning att obetydliga intrång ska vara tillåtna.

Rekvisitet "inte … obetydligt intrång i en annan stats suveränitet" är sannolikt inte lätt att tillämpa för svenska domstolar och brottsbekämpande myndigheter. Det är därför viktigt att förarbetena, inklusive regeringens proposition, ger så stor vägledning som möjligt; det är regeringen som är ansvarig för landets internationella förbindelser.

Utredningen skriver att "[t]illgång till uppgifter på ett användarkonto genom inloggning på kontot eller i övrigt normal åtkomst till tjänsten bör som huvudregel anses vara ett obetydligt intrång i andra staters suveränitet" (s 513). Som nämnts ser ett antal andra stater förmodligen saken på ett liknande sätt, men det behöver inte vara så, och olika stater kan ha olika intressen av att skydda olika typer av uppgifter, vare sig det handlar om skydd för privatlivet, för nationell säkerhet eller annat. Risken för att en svensk åtkomst av elektronisk information skulle strida mot lokal lagstiftning diskuteras inte.

Utredningen anför också att det vid avgörandet om ett intrång är obetydligt ska göras en proportionalitetsbedömning (ss 512-513). Det motstående intresse på den andra statens sida som nämns är informationssäkerhet. I detta sammanhang bör följande påpekas. Den svenska lagstiftaren kan sägas förfoga över de värden som ska avgränsas vid en vanlig, "nationell" proportionalitetsavvägning, men den kan inte avgöra vilka intressen som kan vara viktiga för en främmande stats suveränitet, vilket förutom informationssäkerhet också kan handla om integritetsskydd, skydd för nationell säkerhet eller andra värden.

I utredningen refereras uppfattningen från den tidigare Utredningen om hemlig dataavläsning att inhämtning av uppgifter direkt från en annan stat skulle kunna innebära en risk för att den som verkställer åtgärden gör sig skyldig till brott i den andra staten (t.ex. dataintrång) (s 448). Den risken diskuteras emellertid inte i betänkandet.

Utredningen skriver vidare att det "för att hemlig dataavläsning ska få användas beträffande elektronisk information som är eller kan vara lagrad utanför Sverige, [ska vara] en förutsättning [att] någon skada inte får åsamkas heller på det avläsningsbara informationssystem som tillståndet avser." (s 470) Om detta bör vara utgångspunkten bör det definieras vad som avses med skada – hårdvaruskada, temporär eller permanent mjukvaruskada, etc. Uttalandena i lagmotiven om

huruvida, och under vilka förutsättningar, som hemlig dataavläsning ska vara tillåtet är undflyende.[35]

Utredningen gör skillnad mellan data lagrad på en mobiltelefon – t ex en misstänkt persons mobiltelefon – och data lagrad på en server, och utredningen menar att informationsinhämtning – inklusive avlyssning och övervakning – från en mobiltelefon utgör ett betydligt större intrång i territorialstatens jurisdiktion än genomsökning på distans (ss 462, 464, 476). Det förklaras dock inte varför så skulle vara fallet. Det är inte givet att t ex avlyssning eller informationsinhämtning från en telefon vilken tillhör en svensk misstänkt som befinner sig i utlandet skulle utgöra en större intrång i en annan stats suveränitet än t ex genomsökning eller hemlig dataavläsning i ett datanätverk i en annan stat.

Diverse frågor

Enligt utredningen ska inhämtning av information som är lagrad utomlands bara vara tillåtet om det kan ske utan bistånd från en tjänsteleverantör, dvs genomsökning på distans och hemlig dataavläsning.

> Vår ståndpunkt är att exekutiv jurisdiktion bara kan komma i fråga såvitt gäller sådan elektronisk information som de brottsbekämpande myndigheterna utan bistånd från någon utomstående kan skaffa sig tillgång till från en plats där de är behöriga att verka, dvs. främst inom Sverige. En längre gående jurisdiktion skulle riskera att komma i konflikt med folkrätten. (s 461)

Detta bör i så fall framgå av lagstiftningen.

Utredningen menar att det endast är tvångsåtgärder som kan genomföras utan bistånd som är folkrättslig accepterade. Juridiska fakultetsnämnden har svårt att förstå detta kategoriska uteslutande av hjälp av tjänsteleverantörer. Som nämnts är det i själva verket sådant bistånd som står i centrum för såväl det andra tilläggsprotokollet till Budapestkonventionen som EU:s nya e-bevisförordning, liksom f ö den amerikanska CLOUD Act (som nämns på s 452 och 456 f). EU-förordningen nämns på flera stället i betänkandet (bl a s 447), men det är förvånande att den inte diskuteras i utredningens överväganden. Förordningen hade inte antagits när betänkandet lades fram, men den förelåg i utkastform redan 2018. För det första kommer den sannolikt att på ett påtagligt sätt påverka polisens möjligheter att få tillgång till elektronisk information. För det andra verkar det – enligt utredningens ovanciterade analys -- som om e-bevisförordningen strider mot folkrätten, vilket hade varit intressant att skriva ut i klartext, med tanke på att förordningen inte var slutligt antagen när betänkandet lades fram.

Det är mindre lämpligt att i svensk lag skriva att svenska myndigheter över huvud taget får göra "intrång i en annan stats suveränitet." Intrång översätts vanligen med "intrusion" på engelska. I det schweiziska positionspapperet från de ovannämnda FN-diskussionerna anges bl a att

[35] „Vid exempelvis hemlig dataavläsning får tekniska hjälpmedel användas, systemskydd brytas och tekniska sårbarheter utnyttjas om det är nödvändigt. Sådana åtgärder kan, när det gäller information som finns i ett annat land än Sverige, vara förbjudna redan av det skälet att användningen av åtgärden skulle innebära ett för stort intrång i det aktuella landets suveränitet. Men även om bedömningen görs att så inte är fallet, kan åtgärden vara förbjuden eftersom den kan orsaka skada på det informationssystem som tvångsmedlet avser." s 513

> state sovereignty protects information and communication technologies (ICT) infrastructure on a state's territory against unauthorised *intrusion* or material damage. This includes the computer networks, systems and software supported by the ICT infrastructure, regardless of whether the infrastructure is private or public. (UN Doc A/76/136, s 87; kursivering tillagd)

Utredningen föreslår inte att det ska finnas en skyldighet att underrätta den stat där informationen finns lagrad (s 471). Juridiska fakultetsnämnden har inte gjort någon bedömning av i vilken mån direktivet om en europeisk utredningsorder kräver underrättelse. Däremot anser fakulteten att det vore lämpligt att berörd stat, om den kan identifieras, underrättas, särskilt eftersom det råder viss osäkerhet om gränsdragningen mellan vad som är folkrättsenligt och inte.

Avslutningsvis instämmer Juridiska fakultetsnämnden i att ”[o]mfattningen av exekutiv jurisdiktion i förhållande till elektronisk information som är eller kan vara lagrad utanför Sverige bör klargöras genom att förutsättningarna framgår av lag” (s 471). Som framkommit ovan finns det ett stort antal aspekter av denna fråga – de flesta av dem ännu outredda -- som det är svårt för en domstol att kunna beakta. (Det HD-beslut som kom i mars d å bekräftar f ö detta omdöme.)

Konsekvenser

Det finns inga närmare överväganden vad gäller andra staters reaktioner eller andra staters reciproka agerande. Skulle Sverige acceptera att andra länder, i jakt på hädare eller dissidenter, 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 eller att de hackar sig in på ett sätt som blott skulle utgöra ett ”obetydligt intrång” i svensk suveränitet?

Som nämnts ovan kan svenska utredningsåtgärder som sker i enlighet med utredningens för-slag eventuellt bedömas som dataintrång i andra länder, vilket i så fall kan utsätta svenska utredare för risker. Här påstås inte att den faran är stor, men risken bör i vart fall bedömas.

Sammanfattande synpunkter

Den folkrättsliga undersökningen är direkt undermålig och måste göras om, vilket är olyckligt, eftersom det, som utredningen framhåller, finns ett stort behov av att brottsbekämpande myndigheter får tillgång till information som finns lagrad utomlands. Vid fortsatt utredning och beredning är det viktigt att folkrättsligt sakkunniga deltar i arbetet samt att Utrikesdepartementet konsulteras.

Vidare finns ett antal oklarheter, bl a följande. Resonemangen om vad som kan tänkas utgöra ett mer än obetydligt intrång i en annan stats suveränitet är outvecklade. Det är oklart varför utredningen inte har sett närmare på frågan om inhämtning av information via tjänsteleverantörer.

3.4 Konsekvenser för företagen

Förslaget innebär omfattande kostnader för de företag som levererar elektroniska kommunikationstjänster och konkurrensnackdelar i ett internationellt perspektiv. Detta får även negativa konsekvenser för konsumenterna av dessa tjänster.

Juridiska fakultetsnämnden delar emellertid inte utredningens uppfattning att den rådande modellen för kostnadsfördelning bör bibehållas. Det innebär i så fall en olikbehandling i förhållande till en lång rad andra skyldigheter som företag har enligt lag, såsom indrivning av mervärdesskatt, vilket också utförs av företag och innebär avsevärda kostnader för dem utan att någon ersättning lämnas. Det finns inget som talar för att de företag som är leverantörer av elektroniska tjänster ska ha rätt till särskilda subventioner för att anpassa sig till ny lagstiftning när detta inte förekommer på andra områden.

Remissvaret har på fakultetsnämndens uppdrag beslutats av dekanus, professor Jessika van der Sluijs. Yttrandet har beretts av universitetslektor Katarina Fast och professor Pål Wrange. Föredragande har varit Sandra Persson. Yttrandet har expedierats av Juridiska fakultetskansliet.

Jessika van der Sluijs

Sandra Persson