Stockholms universitet

2025-01-17 Dnr SU-3918-24

Juridiska fakultetskansliet Justitiedepartementet

Remiss: Utkast till lagrådsremiss Datalagring och tillgång till elektronisk information

1. Sammanfattning

- Juridiska fakultetsnämnden finner att nationell säkerhetslagring som föreslås i en ny lag om lagring och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet, i och för sig kan utgöra en legitim åtgärd. Hur behovs- och proportionalitetsprinciperna ska upprätthållas beträffande nationell säkerhetslagring är emellertid mindre tydligt. Den föreslagna lagstiftningen balanserar enligt Juridiska fakultetsnämnden på gränsen för det tillåtna, vilket ställer särskilt höga krav på hur beslutsfattandet, förfarandet m.m. utformas. Juridiska fakulteten kan därför i nuläget inte tillstyrka förslaget fullt ut. Om förslaget genomförs bör den nya lagen göras tidsbestämd.
- Juridiska fakultetsnämnden tillstyrker att Säkerhetspolisen ska fatta beslut om nationell säkerhetslagring, men detta bör ske i samråd med Försvarsmakten. Därutöver behöver tidsramarna för beslutet analyseras ytterligare. Ett år framstår som för långt i förhållande till de ingrepp i ett stort antal individers fri- och rättigheter som förslaget innebär, i synnerhet som beslutet kan förlängas.
- Juridiska fakultetsnämnden finner att den föreslagna regleringen rörande ombudsfunktionen bör kompletteras. Det gäller särskilt beträffande krav på ombudets kvalifikationer och att ombudets oberoende ställning behöver stärkas ytterligare. Vidare föreslår Juridiska fakultetsnämnden att en särskild ombudsmannaorganisation bör övervägas.
- Juridiska fakultetsnämnden tillstyrker det förfarande som föreslås men förordar att vissa tillägg görs för att stärka garantierna i förfarandet. Försvarsunderrättelsedomstolens beslut ska vara möjliga att överklaga och en löpande översyn bör ske. Det saknas vidare en närmare analys för vilka möjligheter som enskilda bör ha att få lagringen av personuppgifter kontrollerad. Vidare bör lagringstiderna kortas ned.

Stockholms universitet
106 91 Stockholm

Besöksadress:
Universitetsvägen 10 A

- Juridiska fakultetsnämnden tillstyrker att en teknikanpassning av lagstiftningen införs, vilken innebär att nummeroberoende interpersonella kommunikationstjänster (Noik) inkluderas. Det finns emellertid en risk för 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. Det framgår inte av förslaget hur det ska hanteras.
- Juridiska fakultetsnämnden vill framhålla att förslaget rörande anpassningsskyldigheten bör analyseras närmare rörande maskin-till-maskin tjänster samt förtydligas vad gäller kryptering, särskilt totalsträckskryptering.

2. Övergripande synpunkter på förslaget

I det förslag som presenteras i utkastet till Lagrådsremiss har delar av det ursprungliga förslaget av Datalagringskommittén arbetats om och preciserats. Utkastet tar dels sikte på att utvidga befintliga krav på datalagring på ett antal områden, såsom att inkludera Noik, dels på att införa en ny möjlighet till nationell säkerhetslagring i en ny lag.

Juridiska fakultetsnämnden kan inte tillstryka hela förslaget utan endast delvis. Nedan presenteras flera synpunkter och förslag. I övrigt hänvisas till Juridiska fakultetsnämndens remissyttrande över 2021 års datalagringsutredning (SOU 2023:22).

Det behöver inte närmare kommenteras att Sverige idag står inför både kända och oanade hot mot den nationella säkerheten. Om detta vittnar inte minst den senaste tidens händelser beträffande sabotage mot undervattenskablar för internettrafik i Östersjön. Polismyndigheter och underrättelsetjänster behöver ges de förutsättningar som krävs för att kunna utföra sina uppgifter i takt med teknikutvecklingen inom ramen för vad som kan anses nödvändigt i ett demokratiskt samhälle och proportionerligt.

Vad som kan betecknas som ett extraordinärt förlopp i form av ett allvarligt hot mot nationell säkerhet bör också behandlas som just detta och inte permanentas.[1] I denna del bör också traditionella principer för krislagstiftning beaktas för att säkerställa att så inte blir fallet.[2] En annan sak är att ett extraordinärt skeende kan pågå under en längre tidsperiod. Som utkastet lyfter fram, går det ju till exempel inte att förutse hur lång tid en förhöjd hotbild dröjer sig kvar, likt den aktuella situationen som Sverige nu befinner sig i. Icke desto mindre måste det aktuella systemet byggas på så sätt att de åtgärder som föreslås inte övergår i ett normaltillstånd och öppnar upp för en rutinmässig massövervakning som därutöver kan vara ineffektiv. I det sammanhanget är det värt att nämna några varnande ord ur FN:s högkommissaries för mänskliga rättigheter rapport *The right to privacy in the digital age* (2022, p. 55):

"Measures of surveillance that are incompatible with international human rights law are already widespread. Even where surveillance serves legitimate purposes, the underlying infrastructure can be easily repurposed, oftentimes serving ends for which it was not originally intended (so-called "function creep") or following changes in the political landscape. Decision makers should keep this in mind when considering new projects that enhance powers to collect and analyse personal data…"

[1] 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.

[2] Se t.ex. Cormacain, Ronan (2020*): Keeping Covid-19 emergency legislation socially distant from ordinary legislation: principles for the structure of emergency legislation,* The Theory and Practice of Legislation, DOI: 10.1080/20508840.2020.1786272

Det förfarande som inrättas enligt förslaget ger enligt Juridiska fakultetsnämnden bättre skydd för fri- och rättigheter och missbruk av systemet än det ursprungliga förslaget av Datalagringsutredningen. Frågan är om det ger tillräckliga garantier och i vilken mån det kan förstärkas ytterligare. Yttermera är det angeläget att resurserna fördelas på så sätt att de brottsbekämpande myndigheterna kan bedriva ett effektivt arbete, där redan beprövade arbetsmetoder och verktyg inte undan vidare bör prioriteras ned eller bort. Juridiska fakultetsnämnden lämnar vissa förslag nedan.

3. Förlängd lagringstid för uppgifter om abonnemang och förtydliganden om vissa regler

Abonnemangsuppgifter urskiljs särskilt i förslaget och bedöms kunna vara föremål för en mer omfattande lagring på grund av sin karaktär som mindre ingripande för den personliga integriteten.

Hur abonnemangsuppgifter definieras i förhållande till trafik- och lokaliseringsuppgifter är en central fråga om förslaget genomförs. Några kriterier som bör uppfyllas för att en abonnemangsuppgift ska föreligga ges emellertid inte i förslaget, vilket framstår som en brist i förslaget.

Regeringen menar att anpassningsskyldigheten inte bör omfatta maskin-till-maskin tjänster. Juridiska fakultetsnämnden menar att det är viktigt att ha en lagstiftning som så långt som möjligt är i takt med teknikutvecklingen. Det borde vara möjligt att göra en rimlig avgränsning i det här avseendet, åtminstone avseende vissa sådana tjänster som, t.ex. rörande vissa fordon. Eftersom det får anses angeläget att hot och brott mot den nationella säkerheten kan avvärjas och bekämpas, framstår det inte som rationellt att inte inkludera några sådana tjänster från vilka de brottsbekämpande myndigheterna finner sig behöva kunna samla in data.

4. Nya regler om datalagring i syfte att skydda nationell säkerhet

Nationell säkerhetslagring, legitimitet och proportionalitet

Datalagring i syfte att skydda nationell säkerhet kan vara en legitim åtgärd som kan rättfärdiga inskränkningar i fri- och rättigheter. En central fråga är därför vilka inskränkningar som är förenliga med proportionalitets- och behovsprinciperna. En inte oviktig fråga i sammanhanget är därför hur effektiv den masslagring som föreslås i själva verket är, såsom t.ex. lyfts fram av Europarådets parlamentariska församling i dess resolution 2045 (2015) om massövervakning (§ 11):

> *”The Assembly recognises the need for effective, targeted surveillance of suspected terrorists and other organized criminal groups. Such targeted surveillance can be an effective tool for law enforcement and crime prevention. At the same time, it notes that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.”*

Det är inte heller klart att kommunikation mellan de aktörer som utgör ett hot mot Sveriges säkerhet, t.ex. en spionring eller en terroristgrupp, sker via vare sig vanliga mobiltelefoner eller sedvanliga Noik, såsom WhatsApp. Det visar t.ex. fallet med kommunikationstjänsten Encrochat, vilken i stor utsträckning användes av organiserad brottslighet och som Juridiska fakultetsnämnden redogjorde för i sitt remissyttrande över

SOU 2023:22 Datalagring och åtkomst till elektronisk information (Dnr SU FV-2740-23). Detta måste också tas i beaktande.

Vidare kan krav på att tillhandahålla bakdörrar och nyckeldeponering avseende totalsträckskrypterade tjänster få motsatt effekt, eftersom det inte bara är brottsbekämpande myndigheter som kan göra bruk av dessa utan även kriminella och andra hotaktörer. Detta påpekades t.ex. av Europol och EU:s cybersäkerhetsmyndighet ENISA i ett gemensamt yttrande 2016:

> *"While no practical encryption mechanism is perfect in its design and implementation, decryption appears to be less and less feasible for law enforcement purposes. This has led to proposals to introduce mandatory backdoors or key escrow to weaken encryption. While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow."*[3]

Juridiska fakultetsnämnden återkommer till frågan om totalsträckskryptering nedan vid genomgången av förslaget kring anpassningsskyldigheten.

Vidare bör riskerna för infiltration hos tjänsteleverantörerna som utför datalagringen för statens räkning beaktas. Om infiltration förekommer, kan det påverka den nationella säkerhetslagringens effektivitet och kan i sin tur få effekter på bevisvärdet hos den data som hämtas in. Frågan är hur väl Säkerhetspolisen kan förlita sig på inhämtad information om det finns risk för att uppgifter förvanskats eller förstörts på grund av detta. Frågan har även betydelse för allmänhetens förtroende för åtgärden och de risker som det kan innebära för fri- och rättigheter om myndigheterna agerar på felaktig information.

Nationell säkerhetslagring har sin grund i ett angeläget allmänt intresse och kan därför generellt anses utgöra en legitim åtgärd. Det står däremot inte lika klart att denna masslagring är nödvändig och proportionerlig. I förslaget lyfts det aktuella säkerhetsläget fram som ett argument. Vidare framställs behovet relaterat till att Säkerhetspolisen får in få anmälningar och att tyngdpunkten i dess arbete därför ligger på underrättelseverksamheten. Det anges också att de aktörer som är föremål för Säkerhetspolisens utredningar är kvalificerade och många gånger har goda kunskaper om hur man döljer digitala spår.[4] Det framgår emellertid inte mer specifikt på vilket sätt en nationell säkerhetslagring kommer att råda bot på detta. I utkastet lyfts fram att det handlar om möjligheter att inhämta trafik- och lokaliseringsuppgifter "förväntas" bidra till myndigheternas arbete med att skydda den nationella säkerheten på ett sådant sätt att det finns ett faktiskt behov att nationell säkerhetslagring införs i svensk rätt. Detta utgör enligt regeringen" i sig ett godtagbart skäl för att begränsa enskildas fri- och rättigheter enligt svensk och europeisk rätt. Därutöver antas förslaget innebära en ökad rättstrygghet för enskilda.[5] Av detta kan utläsas att det inte handlar om att det föreligger några bevis för att nationell säkerhetslagring behövs utan snarare om förväntningar på vad nationell säkerhetslagring ska bidra med till underrättelseverksamheten.

---

[3] *On lawful criminal investigation that respects 21st Century data protection*. Europol and ENISA Joint Statement 20 May 2016.

[4] Utkast till Lagrådsremiss, s. 40 f.

[5] Utkast till Lagrådsremiss, s. 41.

För att avgöra om åtgärden är proportionerlig framstår det också som nödvändigt att bedöma hur nationell säkerhetslagring förhåller sig och samspelar med andra åtgärder som står till buds, såsom hemlig dataavläsning.

Mot bakgrund härav framstår det som oklart om nationell datalagring som sådan är en nödvändig och effektiv åtgärd för att avvärja hot och bekämpa brott mot nationell säkerhet. Det innebär, om lagen införs, att Sverige balanserar på gränsen för vad som är tillåtet, i synnerhet i förhållande till skyddet för privatlivet. Det ställer höga krav både på det förfarande som föreslås och tillämpningen av lagen.

Detta talar vidare för att dessa bestämmelser bör göras tidsbegränsade för att avgöra om den nationella säkerhetslagringen uppfyller de förväntningar som föreligger, i vilken mån det handlar om ett nödvändigt och proportionerligt ingrepp i mänskliga fri- och rättigheter, men också om den nationella säkerhetslagringen bidrar till en rationell resursfördelning i underrättelsearbetet i praktiken.

Beslut om nationell säkerhetslagring

Juridiska fakultetsnämnden finner att det är rimligt att Säkerhetspolisen beslutar om det föreligger ett allvarligt hot mot Sveriges säkerhet och det är absolut nödvändigt att förelägga leverantörer att vidta en mer omfattande lagringsskyldighet. Juridiska fakultetsnämnden finner emellertid i likhet med Datalagringsutredningen att det normalt bör föreligga en samrådsskyldighet med Försvarsmakten. Detta då det föreligger höga krav på behovet av en utökad lagringsskyldighet.

Juridiska fakultetsnämnden förordar utkastets förslag att kravet på att en proportionalitetsbedömning explicit bör komma till uttryck i lagtexten. Bedömningen om fråga är om ett ”allvarligt hot mot Sveriges säkerhet” och när det är ”absolut nödvändigt” att besluta om ett sådant föreläggande är svårt att avgöra på förhand. Viss vägledning finns redan i den praxis om massövervakning och datalagring som utarbetats inte minst i Europadomstolen och EU-domstolen samt lagförarbeten. På sikt kan en nationell praxis rörande tillämpningen av dessa rekvisit i den föreslagna lagstiftningen utkristalliseras som härefter kan bli föremål för utvärdering. I inledningsskedet är det därför av stor betydelse hur förfarandet kring detta beslut sker. Av denna anledning finner Juridiska fakultetsnämnden att ett beslut av Säkerhetspolisen i samråd med Försvarsmakten är av betydelse.

Enligt utkastet ska förslaget gälla i ett år. Möjligen bör denna tid begränsas till sex månader i taget med tanke på den inskränkning som lagringen innebär för fri- och rättigheter. Det är förvisso, som lyfts fram i utkastet, så att den art av brottslighet som Säkerhetspolisen utreder pågår under lång tid. Det framstår emellertid inte som om detta bör vara styrande, dels då detta inte kan vara typiskt enbart för brott mot nationell säkerhet och att nationell säkerhetslagring i sådana fall skulle behöva ske under en betydligt längre tid än endast ett år. I det här avseendet påkallar fri- och rättighetsskyddet en kortare beslutstid. Enligt förslaget finns ju inte någon gräns för hur många gånger som beslutet kan förlängas, vilket innebär att lagringen kan ske så länge som det är nödvändigt och proportionerligt.

Domstolskontroll och regler om ombud

Juridiska fakultetsnämnden instämmer med förslaget i utkastet att Försvarunderrättelsedomstolen ska vara kontrollorgan. I övrigt hänvisar till Juridiska fakultetsnämnden till sitt remissyttrande rörande SOU 2023:22.

Juridiska fakultetsnämnden förordar de bestämmelser om ombud som föreslås som helhet men har vissa synpunkter.

Med tanke på de kvalificerade bedömningar som det här är fråga om, vilka har en mycket stor betydelse för enskildas fri- och rättigheter avseende en stor del av den svenska befolkningen, finns det skäl att ställa särskilt höga krav på ombudets kvalifikationer och omdöme. Det bör därför vara särskilt kvalificerade jurister med processvana som bör komma ifråga, det vill säga personer med bakgrund som advokat eller ordinarie domare.

Det ställer vidare stora krav på en oberoende ställning i förhållande till regeringsmakten. Det framstår därför som mindre lämpligt att regeringen utser ombudet. Den ordning som föreslås innebär ett tämligen stort skön för regeringen att utse personer som regeringen finner tillräckligt kvalificerade och inom en begränsad tidsperiod om endast 3 år. Om regeringen ska utse ombud måste det vara ett krav att det i så fall endast sker utifrån den krets av personer som föreslås av Sveriges Advokatsamfund och Domarnämnden. Dessa organisationer får antas bäst kunna bedöma ombudets kvalifikationer. En alternativ ordning är att regeringen inte utser ombudet utan att detta görs av Riksdagen.

Juridiska fakultetsnämnden finner att ombudet bör utnämnas för en längre tidsperiod än tre år, förslagsvis minst fyra år. Detta för att bättre säkerställa oberoendet hos ombudet. Det framgår i vart fall inte varför det ska föreligga en annan ordning än för Integritetsskyddsombud, som utses för fyra år i taget.

Det finns även skäl att närmare överväga Uppsala universitets remissyttrande avseende SOU 2023:22 i denna del, i vilket det diskuteras om det är lämpligt att knyta ansvaret till en enda persons omdöme. Detta bör i vart fall tillgodoses så att ombudet får tillräckligt med resurser till sitt förfogande för att utföra sitt uppdrag.

En alternativ ordning skulle kunna vara att inrätta en ombudsorganisation, i vilken integritetsskyddsombuden enligt lagen (2009:966) om Försvarsunderrättelsedomstol skulle kunna integreras. På så vis kan ombud utses som kan agera ombud både beträffande ärenden om signalspaning och nationell säkerhetslagring.

Förfarandet och lagringsskyldighetens omfattning

Juridiska fakultetsnämnden tillstyrker att förfarandet utformas på så sätt att Säkerhetspolisens beslut omedelbart underställs Försvarsunderrättelsedomstolen samt att Försvarsunderrättelsedomstolen beslutar om ersättning till ombudet.

Juridiska fakultetsnämnden delar emellertid den uppfattning som framförts i flera remissyttranden över Datalagringsutredningens förslag av t.ex. Sveriges Advokatsamfund, Sveriges Domareförbund och Svenska Journalistförbundet, att Försvarsunderrättelsedomstolens beslut ska vara möjliga att överklaga samt att en löpande översyn sker. Det saknas vidare en närmare analys för vilka möjligheter som enskilda bör ha för att kunna få lagringen av personuppgifter kontrollerad.

Juridiska fakultetsnämnden finner att de tider för masslagring som föreslås är för långa i förhållande till det ingrepp som de utgör i individers fri- och rättigheter. Lagringstiderna bör halveras.

5. Nya regler för tillhandahållande av nummeroberoende interpersonella kommunikationstjänster

Inkludering av Noik

Juridiska fakultetsnämnden tillstyrker att en teknikanpassning av lagstiftningen införs, vilken innebär att Noik inkluderas. Det föreligger emellertid, såsom Juridiska fakulteten tidigare har lyft fram i sitt remissyttrande till SOU 2023:22, en risk att denna teknikanpassning inte får den effekt som eftersträvas. Detta hänger samman med att de företag som tillhandahåller dessa tjänster till stor del är belägna utanför EU. Det är inte självklart att de kommer att kunna hörsamma lagrings- och anpassningskrav från svenska myndigheter på samma sätt som svenska företag.[6]

Det framgår inte av vare sig det nu aktuella eller det tidigare förslaget hur denna problematik ska hanteras. Ska Sverige söka genomdriva bilaterala handräckningsavtal med de länder där det förekommer företag som tillhandahåller Noik? Ett problem härvidlag kan till exempel vara att alla dessa stater inte är demokratiska rättsstater som respekterar mänskliga rättigheter.

Sverige kan driva dessa frågor inom EU och internationellt vilket på sikt kanske kan bidra till att en tillfredsställande internationell reglering av området införs. Detta synes emellertid inte vara möjligt inom en nära framtid. I övrigt hänvisar Juridiska fakultetsnämnden till de särskilda synpunkter och kommentarer rörande dessa folkrättsliga frågor som lämnades i remissyttrandet till SOU 2023:22.

Anpassningsskyldighet

Ovan redogjordes kort för att kryptering och särskilt totalsträckskryptering kan anses vara väsentligt för att skydda känsliga kommunikationer och rätten till privatliv. Frågan är om det kan anses utgöra ett en del av anpassningsskyldigheten att t.ex. utforma bakdörrar för att möjliggöra dekryptering av kommunikation.

När det gäller kryptering kan detta vara en väsentlig åtgärd för att säkerställa en hög nivå av såväl informations- som cybersäkerhet. Det finns rättsliga bestämmelser som explicit nämner kryptering såsom i artikel 32 (1a) i den allmänna dataskyddsförordningen och artikel 21 (2h) i NIS2-direktivet. I skäl 98 till NIS2-direktivet, som också hänvisas till i utkastet till Lagrådsremiss lyfts särskilt fram att:

> *”För att trygga säkerheten för allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av krypteringsteknik främjas, särskilt totalsträckskryptering… Vid behov bör användningen av kryptering, särskilt totalsträckskryptering, vara obligatorisk för tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt inbyggt integritetsskydd vid tillämpningen av detta direktiv. Användningen av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra förebyggande utredning, upptäckt och lagföring av brott i enlighet med unionsrätten. Detta bör dock inte försvaga totalsträckskrypteringen, som är en kritisk teknik för ett effektivt dataskydd, integritet och kommunikationssäkerhet.”*

[6] 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.

Skäl 98 i NIS2-direktivet ger inte något svar på hur långt anpassningsskyldigheten sträcker sig i det aktuella hänseendet, även om det står klart att totalsträckskryptering utgör en kritisk teknik.

Problemen rörande totalsträckskryptering (*end-to-end encryption*), som förekommer i vissa Noik-tjänster, kan vara särskilt allvarliga från ett människorättsperspektiv.[7] I detta sammanhang är Europadomstolens dom i *Podchasov ./. Ryssland* från den 13 februari 2024 av särskilt intresse, vilken emellertid inte synes ha analyserats i utkastet till Lagrådsremiss.

Frågan i målet var om rysk ”informationslagstiftning” som var tillämplig på kommunikationstjänsten Telegram Messenger var förenlig med artikel 8 i Europakonventionen om skydd för privat- och familjeliv, hem och korrespondens. Lagen innebar ett omfattande krav på datalagring hos tjänsteleverantörerna, närmare bestämt att all data rörande internettrafik skulle lagras i sex månader och alla relaterade kommunikationsdata i ett år. Lagen innebar vidare att underrättelsetjänsten FSB kunde göra anspråk på direktåtkomst till denna data. Ytterligare förelåg en skyldighet för leverantörerna att dekryptera totalsträckskrypterad kommunikation genom nyckeldeponering. Det sistnämnda kravet skulle innebära att all kommunikation för alla användare av tjänsten skulle dekrypteras och inte endast de konton som ryska FSB ville undersöka.

Telegram vägrade att efterkomma FSB:s krav av framför allt detta skäl och tjänsten förbjöds senare under två år i Ryssland.

Europadomstolen fann att den ryska lagstiftningen inte var förenlig med artikel 8, då den inte kunde anses nödvändig i ett demokratiskt samhälle. Detta, då den ger myndigheterna en generell tillgång till innehåll av elektroniska kommunikationer, utan att det föreligger några garantier för att upprätthålla individuella rättigheter. *”It impairs the very essence of the right to respect of private life under Article 8 of the Convention.”* (§ 80). Vad som är av särskilt intresse avseende det aktuella förslaget är att Europadomstolen i domen uttalar en tämligen tydlig gräns för hur data från Noik kan användas av svenska myndigheter i förhållande till totalsträckskryptering. Europadomstolen konstaterar att för att kunna dekryptera vissa meddelanden i Telegrams kommunikationstjänst, så måste krypteringen för alla användare försvagas, vilket öppnar upp för FSB att utföra en rutinmässig, generell och urskillningslös övervakning av privat elektronisk kommunikation. Detta kan enligt domstolen inte anses proportionerligt (§ 79). Om det däremot finns alternativa tekniska lösningar för att dekryptera kommunikationer utan att krypteringens skyddande mekanismer försvagas, skulle en annan bedömning kunna göras (§ 78).[8]

I utkastet till Lagrådsremiss anges att förslaget ”i sig inte innebär att någon generell sårbarhet ska införas i kryptering eller att systematiska bakdörrar introduceras”. Det hänvisas härefter till att utredningen anger att det är ”fullt möjligt för tillhandahållare av Noik att utforma sina tjänster så att kraven på säkerhet och skyddet för kommunikation

[7] Se t.ex. FN:s högkommissaries för mänskliga rättigheter rapport *The right to privacy in the digital age* (2022), § 23.

[8] För en kommentar till domen i Podchasov se vidare Shurson, Jessica, *A European right to end-to-end encryption?* Computer Law & Security Review 55 (2024).

tillgodoses”. Den närmare skyldigheten om vad som kan krävas beträffande tekniska lösningar får enligt utkastet avgöras vid tillämpningen och i rättspraxis.[9]

Det bör därför tydligare framgå i regeringens förslag ett det inte faller inom ramen för anpassningsskyldigheten att dekryptera totalsträckskrypterad kommunikation i en viss kommunikationstjänst om det innebär en försvagning i krypteringen för samtliga eller en stor del av användarnas kommunikation och några andra tekniska lösningar inte står till buds.

Remissvaret har på fakultetsnämndens uppdrag beslutats av dekanus, professor Jane Reichel. Yttrandet har beretts av universitetslektor Katarina Fast Lappalainen. Föredragande har varit utredare Karolina Alveryd. Yttrandet har expedierats av Juridiska fakultetskansliet.

Jane Reichel

Karolina Alveryd

[9] Utkast till Lagrådsremiss, s. 88.