2026-11-04

Justitiedepartementet
103 33 Stockholm

Yttrande/Remiss över SOU 2026:45 ”Effektiva ingripanden mot brott i cybermiljö”, Ju2026/01670

Beredda möjlighet därtill lämnar 5 Juli-stiftelsen (”Stiftelsen”) följande remissvar:

Stiftelsen konstaterar att utredningen inte håller sådan kvalitet att den kan ligga till grund för lagstiftning. De befogenheter som utredaren föreslår att svenska myndigheter ska ges – att genomföra dataintrång, bereda sig tillgång till information i enskildas informationssystem samt ändra, blockera och radera uppgifter – är mycket långtgående. Samtidigt är de begränsningar av myndigheternas befogenheter som föreslås otillräckliga för att ge enskilda ett godtagbart skydd mot godtycke och missbruk.

Utredningen uppvisar också betydande brister när det gäller att beskriva och värdera de konsekvenser som förslagen skulle få för enskilda, företag och samhället i stort. I synnerhet har konsekvenserna för säkerheten på internet och den infrastruktur som stora delar av det svenska samhället är beroende av inte analyserats på ett adekvat sätt. Inte heller har utredaren visat att de befogenheter som föreslås skulle få de positiva effekter för brottsbekämpningen som anförs i stöd för dem.

Stiftelsen menar vidare att utredningen inte visar att förslaget uppfyller de grundläggande kraven på skydd för privatliv, korrespondens samt yttrande- och informationsfrihet som följer av regeringsformen (RF) och Europakonventionen om de mänskliga rättigheterna (EKMR).

Stiftelsen menar att det, i stället för att ytterligare en lag som ger svenska myndigheter långtgående befogenheter att övervaka enskilda och göra intrång i deras informationssystem införs, finns anledning att genomföra en samlad översyn av de befogenheter som myndigheterna redan har. Vid en sådan översyn bör en nyttokostnadsanalys göras som även omfattar kostnaderna för övervakningen och konsekvenserna för säkerheten i de informationssystem som används av privatpersoner, företag och myndigheter.

Det bör här även utredas i vilken utsträckning brottslighet skulle kunna förhindras genom att säkerheten i informationssystem stärks snarare än genom att staten ges utökade möjligheter att göra intrång i dem. Stiftelsen menar att det är en viktig uppgift för staten att skydda svenskarna och svenska företag från dataintrång och andra angrepp mot deras informationssystem.

Med hänvisning till ovanstående *avstyrker* Stiftelsen förslaget.

Erik Lakomaa,

Ordförande 5 juli-stiftelsen

Nedan utvecklas grunderna för Stiftelsens ställningstagande.

Bakgrund och allmänt om utredningen

Under de senaste regeringsperioderna har en rad offentliga utredningar om statens befogenheter att övervaka svenskarna och deras kommunikationer genomförts. Gemensamt för dessa har varit att de i princip samtliga funnit att de befogenheter som myndigheterna vid respektive tillfälle haft inte varit tillräckliga och att de föreslagna utökningarna av befogenheterna varit nödvändiga och proportionerliga. Detta även när myndigheterna alldeles nyligen har fått nya befogenheter och det ännu inte har varit möjligt att utvärdera dessa.

Någon samlad analys av konsekvenserna av den övervakning som redan sker, eller av de sammantagna konsekvenserna av de förslag som har lagts fram i olika utredningar, har inte genomförts. Inte heller har någon adekvat nyttokostnadsanalys av den statliga övervakningen genomförts.

Denna utredning skiljer sig i dessa avseenden inte nämnvärt från tidigare utredningar inom övervakningsområdet. Det som däremot skiljer förslaget från flera tidigare förslag är att utredaren inte nöjer sig med att myndigheter ska kunna bereda sig tillgång till information i människors privata informationssystem. Myndigheterna ska också få möjlighet att ändra och blockera information och, i vissa fall, förstöra den. Utredaren föreslår också att myndigheter ska kunna bereda sig tillgång till trafikuppgifter under befordran till eller från vissa informationssystem för att kartlägga kommunikation med andra system. Därutöver ska myndigheterna i vissa situationer kunna bereda sig tillträde till platser som annars är skyddade mot intrång för att installera tekniska hjälpmedel. Det är således fråga om befogenheter som sammantaget går betydligt längre än vad som normalt avses med övervakning. Staten ska inte bara kunna få tillgång till information, utan också kunna påverka den information människor har tillgång till och de informationssystem som de använder.

Stiftelsen menar att det, med tanke på hur långtgående befogenheterna är, finns anledning att ställa synnerligen höga krav på utredningen, både när det gäller att visa behovet av befogenheterna och när det gäller att beskriva deras konsekvenser. Utredningen lever inte upp till dessa krav.

Stiftelsen konstaterar att utredaren redovisar uppskattningar av de kostnader som de nya befogenheterna skulle medföra för de brottsbekämpande myndigheterna, åklagarväsendet och tillsynsmyndigheten. Detta är emellertid inte detsamma som att de samlade kostnaderna för lagstiftningen har analyserats. Utredaren berör i begränsad utsträckning de kostnader som ingripandena skulle kunna medföra för enskilda, företag och samhället i stort. Någon tillräckligt utvecklad analys av exempelvis kostnaderna för skador på informationssystem, avbrott i tjänster eller de ökade säkerhetsriskerna som användningen av sårbarheter kan medföra görs inte.

Utredaren gör samtidigt bedömningen att de föreslagna befogenheterna kommer att ha positiva effekter för små företags arbetsförutsättningar. När det gäller barn görs bedömningen att

förslagen inte får några särskilda konsekvenser, trots att utredaren själv konstaterar att unga i särskilt stor utsträckning använder cybermiljön och att de kan påverkas mer negativt än vuxna av att utsättas för ingripanden. Stiftelsen menar att dessa bedömningar är otillräckligt underbyggda.

Det är knappast rimligt att anta att en lagstiftning som ger myndigheter rätt att göra intrång i människors privata informationssystem och ändra eller förstöra information skulle sakna särskilda konsekvenser för exempelvis barn och unga. Inte heller kan det utan vidare antas att små företag skulle gynnas av lagstiftningen om de samtidigt riskerar att drabbas av ingripanden mot system som de själva eller deras leverantörer använder. För att kunna göra en proportionalitetsbedömning är det nödvändigt att kostnaderna för lagstiftningen beskrivs. Att dessa kostnader är svåra att kvantifiera innebär inte att de får bortses ifrån.

En proportionalitetsbedömning som utgår ifrån att nyttorna är omfattande medan kostnaderna är begränsade, utan att det finns tillräckligt underlag för något av dessa antaganden, kan inte ligga till grund för så långtgående inskränkningar av människors fri- och rättigheter som de föreslagna.

För att en åtgärd överhuvudtaget ska kunna vara proportionerlig krävs att den kan förväntas uppnå det syfte som anförs till stöd för den. Vidare krävs att nyttorna av åtgärden överstiger kostnaderna och att motsvarande nyttor inte kan uppnås till lägre kostnader – ekonomiska eller andra – på något annat sätt. För att kunna avgöra om så är fallet krävs att både nyttor och kostnader identifieras och, i den mån det är möjligt, kvantifieras. Att beskriva ett antal angelägna samhällsproblem och därefter konstatera att de befogenheter som myndigheterna efterfrågar är proportionerliga i förhållande till dessa problem kan inte betraktas som en fullgod proportionalitetsbedömning.

Stiftelsen ifrågasätter inte att den brottslighet som utredaren beskriver utgör ett samhällsproblem. Att ett samhällsproblem föreligger innebär dock inte att varje åtgärd som påstås kunna bidra till att lösa problemet faktiskt gör det. Utredaren beskriver i avsnitt 12.4 ett antal situationer där myndigheterna anser sig behöva kunna ingripa i informationssystem. Utredningen utgår i betydande utsträckning från att nya rättsliga befogenheter också kommer att innebära en väsentligt effektivare brottsbekämpning. Det framgår emellertid inte i vilken utsträckning myndigheterna i de beskrivna situationerna faktiskt har haft tekniska möjligheter att genomföra ingripanden, men har hindrats av att lagstöd saknats. Det är fullt möjligt att de hinder som myndigheterna möter i betydande utsträckning är av teknisk snarare än juridisk natur.

Att myndigheter genom lag ges rätt att göra intrång i ett informationssystem innebär exempelvis inte att de får tekniska möjligheter att göra det. Det innebär inte heller att myndigheterna får möjlighet att identifiera var ett informationssystem finns, hur det kan nås eller vem som kontrollerar det. En lag som ger staten rätt att göra något som den inte har praktisk möjlighet att göra kan inte motiveras med att den skulle vara ett effektivt verktyg.

Inte heller innebär ett i teknisk mening framgångsrikt ingripande med nödvändighet att någon brottslighet förhindras. Om myndigheterna exempelvis lyckas stänga ner en tjänst som används för försäljning av narkotika kan det förstås innebära att försäljningen via den aktuella tjänsten

upphör. Det innebär dock inte att försäljningen av narkotika upphör. Försäljarna kan använda andra tjänster eller försäljningskanaler. Utredningen berör i sin konsekvensanalys möjligheten att viss brottslighet flyttas till andra länder. Det visar emellertid inte att brottsligheten minskar totalt sett. Inte heller redovisas något tillräckligt underlag för att kunna bedöma hur stor del av de förväntade effekterna som består i att brottsligheten förhindras respektive flyttas till andra tjänster, infrastrukturer eller geografiska områden.

Det är anmärkningsvärt att utredaren gör bedömningen att lagen kommer att ha en avhållande effekt på brottsligheten och att vissa brottsfenomen kan förväntas minska avsevärt, utan att dessa slutsatser underbyggs med någon tydligt redovisad empirisk analys.

Stiftelsen menar, liksom i tidigare remissvar, att bevisbördan när det gäller de påstådda nyttorna av inskränkningar av människors fri- och rättigheter måste ligga på den som föreslår inskränkningarna. Det kan inte ankomma på dem som vill värna de grundläggande fri- och rättigheterna att visa att inskränkningar av dessa inte skulle ge de nyttor som utredaren påstår.

Utredaren motiverar i stor utsträckning de föreslagna befogenheterna med förekomsten av mycket allvarlig brottslighet. Till de exempel som ges hör omfattande bedrägerier, organiserad brottslighet, utpressningsangrepp, spridning av skadlig kod, terrorism och angrepp mot samhällsviktig verksamhet. Det kan dock konstateras att de föreslagna befogenheterna inte begränsas till sådan brottslighet.

Enligt 6 § i förslaget till lag om polisiära ingripanden i cybermiljö ska ingripanden kunna ske vid brott för vilka fängelse i ett år eller mer ingår i straffskalan. Som utredaren själv klargör är det tillräckligt att maximistraffet är minst ett års fängelse. Det krävs således inte att det brott som motiverar ingripandet skulle kunna förväntas leda till ett års fängelse, än mindre att minimistraffet för brottet är ett års fängelse. Detta är en viktig distinktion. Även brott för vilka påföljden i normalfallet kan förväntas bli betydligt lindrigare än ett års fängelse kommer därmed att kunna ligga till grund för ingripanden av det slag som föreslås. Utredaren konstaterar också uttryckligen att den valda avgränsningen innebär att i princip samtliga brott som bedöms relevanta i sammanhanget omfattas.

Det kan vidare konstateras att förslaget inte enbart omfattar brott där det digitala informationssystemet utgör målet för brottet, utan även brott som begås *med hjälp av* informationssystem. En betydande mängd traditionell brottslighet kommer därför att kunna omfattas. Det är en sak att diskutera befogenheter som skulle kunna motiveras av exempelvis ett pågående angrepp från en statsaktör mot Sveriges elförsörjning. Det är en annan sak att använda ett sådant angrepp som motivering för befogenheter som också ska kunna användas vid betydligt mindre allvarlig brottslighet, exempelvis vid upphovsrättsintrång.

Att utredaren tänker sig att myndigheterna vid tillämpningen av lagen ska göra en proportionalitetsbedömning löser inte problemet med lagens utformning. Syftet med att i lag begränsa myndigheters befogenheter är rimligen att det inte ska vara myndigheterna själva som avgör hur långtgående deras befogenheter ska vara.

Otydliga förutsättningar för ingripanden

Utredaren använder sig bland annat av begreppet ”brottslig verksamhet” för att beskriva de situationer där myndigheterna kan ingripa. Det innebär att ingripanden i vissa fall ska kunna ske utan att något konkret brott har identifierats. För ingripanden enligt 4 §, som avser tillfällig tillgång till trafikuppgifter under befordran, krävs att det kan antas att ett informationssystem används vid brott eller brottslig verksamhet. Utredaren klargör att detta krav är avsett att vara lågt ställt. För ingripanden enligt 3 och 5 §§ finns däremot inget motsvarande uttryckligt krav på misstanke om, eller risk för, att just det informationssystem som berörs används eller kommer att användas vid brottslighet. I stället ska det vara av särskild respektive synnerlig vikt att ingripandet görs för det angivna ändamålet. Det innebär att en betydande del av avgränsningen överlåts till den myndighet som vill genomföra ingripandet.

Även begreppet ”informationssystem” ges ett mycket vidsträckt tillämpningsområde. Det kan omfatta såväl enstaka uppkopplade enheter som stora och komplexa system med ett stort antal användare. Att brottslig verksamhet kan bedrivas med hjälp av ett informationssystem innebär dessutom inte att informationssystemet har skapats för brottslig verksamhet eller att dess ägare eller övriga användare har någon koppling till brottsligheten. Ett informationssystem kan exempelvis utnyttjas av någon som genom ett dataintrång har tagit kontroll över det. Den som äger systemet är i så fall själv ett brottsoffer. Det skulle med den föreslagna lagstiftningen kunna innebära att den som utsatts för ett dataintrång därefter utsätts för ytterligare ett intrång, denna gång av svenska myndigheter.

Stiftelsen har i tidigare remissvar påtalat problemet med att åtgärder som innebär övervakning av enskilda ges olika beteckningar beroende på vilken myndighet som ska bedriva övervakningen eller vilket syfte som anförs som stöd för den. I denna utredning kallas de åtgärder som myndigheterna ska få vidta för ”ingripanden i cybermiljö”.

Utredaren framhåller att de föreslagna befogenheterna skiljer sig från hemlig dataavläsning bland annat genom att *syftet* är att förhindra, störa eller avbryta brottslighet snarare än att systematiskt samla in information. Utredaren anger också att den nya lagen, som huvudregel, inte är avsedd att ge myndigheterna rätt att kopiera information från ett informationssystem till sina egna system. I författningskommentaren öppnas dock för sådan kopiering om den utgör ett absolut nödvändigt tekniskt steg för att genomföra ingripandet. Ur den enskildes perspektiv torde det emellertid vara av underordnad betydelse, vilket syfte en myndighet uppger sig ha med att bereda sig tillgång till vederbörandes telefon eller dator. Intrånget i privatlivet som sker när en myndighet får tillgång till information i ett privat informationssystem förändras inte av att myndigheten uppger att den inte avser att använda informationen för att utreda brott. Inte heller är det givet att integritetsintrånget blir mindre eftersom intrånget är kortvarigt. På en telefon eller dator kan det finnas kommunikationer, bilder, uppgifter om sjukdomar, ekonomiska förhållanden och andra uppgifter om en persons privatliv som sträcker sig många år tillbaka i tiden. Att det tar kort tid för en myndighet att få tillgång till dessa uppgifter innebär inte att integritetsintrånget är ringa.

Här bör även noteras att utredaren uttryckligen konstaterar att information som blir tillgänglig i samband med ingripanden enligt den nya lagen kan användas i förundersökningar och för att

berika myndigheternas underrättelseverksamhet. Någon särskild reglering av överskottsinformation föreslås inte (s. 341–347). Det innebär att information som myndigheter har fått tillgång till genom att använda de nya befogenheterna kan komma till användning i verksamhet där motsvarande tillgång till information annars skulle ha varit föremål för andra krav och begränsningar (exempelvis advokatsekretess eller källskydd). Därmed finns också en risk att myndigheterna får incitament att använda sina befogenheter för att få tillgång till information som de inte hade kunnat inhämta med stöd av de regler som gäller för hemlig dataavläsning.

Stiftelsen menar att det är de faktiska åtgärder som en myndighet vidtar, och inte vilken beteckning dessa åtgärder ges, som ska avgöra vilka rättssäkerhetsmekanismer som ska omge dem. De begränsningar som införts i lagstiftningen om hemlig dataavläsning kan inte rimligen vara avsedda att endast gälla så länge myndigheterna själva väljer att kalla de åtgärder de vidtar för hemlig dataavläsning.

Förslaget uppfyller inte de grundläggande kraven på skydd för privatlivet

Enligt artikel 8 i EKMR har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Skyddet för den personliga integriteten finns också i 2 kap. RF.

Stiftelsen konstaterar att utredningen inte på ett tillfredsställande sätt visar hur de långtgående befogenheter som föreslås är förenliga med dessa bestämmelser. Utredaren föreslår visserligen ett antal rättssäkerhetsgarantier. Det finns krav på proportionalitet, särskilda begränsningar för viss skyddad verksamhet och vissa uppgifter, särskilda krav vid radering, dokumentationsskyldighet samt särskild tillsyn. Frågan är emellertid inte om det finns några rättssäkerhetsgarantier, utan om de är tillräckliga med tanke på hur omfattande de föreslagna befogenheterna är.

För att inskränkningar av de rättigheter som skyddas av artikel 8 EKMR ska vara tillåtna krävs det inte bara att de sker med stöd av lag och för något av de ändamål som anges i artikeln, utan också att de är nödvändiga i ett demokratiskt samhälle. Av Europadomstolens praxis framgår vidare att lagstiftning som tillåter hemlig övervakning måste omgärdas av effektiva skyddsmekanismer mot godtycke och missbruk. Utredningens förslag uppfyller inte dessa krav.

Att en lagstiftning uppfyller de grundläggande kraven på skydd för mänskliga rättigheter som följer av EKMR och RF kan förvisso inte tas som intäkt för att den är önskvärd eller ens välavvägd. Det måste emellertid betraktas som ett minimikrav för att den ska kunna införas.

Konsekvenser för yttrande- och informationsfriheten

Utredaren föreslår att myndigheter ska få ändra, blockera och i vissa fall radera information i informationssystem. Det är därmed uppenbart att förslaget aktualiserar frågor om yttrande- och informationsfriheten. En stor del av de politiska diskussionerna som idag förs sker på internet. Detsamma gäller organiseringen av politiska aktiviteter, demonstrationer och annan opinionsbildning. De tjänster som används för detta är i stor utsträckning desamma som används för all annan kommunikation och därmed även för kommunikation mellan personer

som ägnar sig åt brottslig verksamhet. Att en viss tjänst används för brottslig verksamhet innebär således inte att de personer som använder tjänsten ägnar sig åt brottslig verksamhet.

Utredaren har förvisso uppmärksammat de grundlagsrättsliga frågorna och föreslår i 8 och 10 §§ särskilda förbud mot ingripanden som riktas mot vissa informationssystem, uppgifter och lokaler som används för skyddad verksamhet (s. 267–275). Detta skydd är emellertid inte generellt. Att vissa yrkesgrupper och verksamheter har ett särskilt skydd innebär inte att andra människors rätt att kommunicera, uttrycka åsikter eller ta del av information får begränsas utan tillräckliga skäl. Det finns dessutom anledning att fråga sig hur skyddet ska fungera i praktiken när myndigheterna inte i förväg vet vilka uppgifter som finns i ett informationssystem och vad de används till.

Stiftelsen menar att det finns betydande risker med att ge myndigheter rätt att blockera eller ändra information i system som används för kommunikation, särskilt när det inte krävs att någon konkret brottsmisstanke föreligger. Vad som skulle hända om myndigheterna på felaktiga grunder kom att uppfatta en laglig politisk verksamhet som brottslig verksamhet är en fråga som borde ha behandlats mer utförligt i utredningen. Det kan exempelvis röra sig om kommunikation mellan personer som organiserar en demonstration och där myndigheterna bedömer att brottslig verksamhet förekommer i anslutning till den aktuella tjänsten eller kommunikationskanalen. Även om det skulle visa sig att ett ingripande som förhindrat kommunikationen varit felaktigt, kan det syfte som kommunikationen skedde för redan ha omintetgjorts. Att i efterhand upphäva ett beslut om att blockera kommunikationen mellan dem som organiserar en demonstration hjälper föga om demonstrationen skulle äga rum dagen innan beslutet upphävdes.

Här bör även konsekvenserna för det journalistiska källskyddet beaktas. För att källskyddet ska fungera krävs det att det finns tillgång till säkra kommunikationskanaler. Det räcker inte att skydda information som omfattas av grundlagsskyddad tystnadsplikt i ett visst informationssystem om en myndighet, genom ett ingripande mot något annat system, kan kartlägga kommunikation eller få tillgång till uppgifter som avslöjar en källa. Stiftelsen menar att lagstiftning som ger staten möjligheter att i hemlighet påverka vilken information människor kan ta del av och vilka kommunikationer som kan äga rum måste omgärdas av synnerligen starka begränsningar. Sådana begränsningar saknas i tillräcklig utsträckning i utredningsförslaget.

Konsekvenser för personer som inte är misstänkta för brott

Utredaren framhåller att ingripandena ska riktas mot informationssystem snarare än mot personer. Detta innebär dock inte att konsekvenserna för enskilda blir mindre. Ett informationssystem kan användas av ett stort antal människor. Ett informationssystem som används av en kriminell aktör behöver inte heller tillhöra denne. Det kan mycket väl vara så att den som äger eller förvaltar informationssystemet själv utsätts för ett brott i form av ett dataintrång. Utredaren uppmärksammar också denna möjlighet, men menar att ingripanden i sådana situationer kan vara positiva för systemets ägare (s. 195f, 259).

Det kan naturligtvis finnas situationer där det är fallet. Det innebär emellertid inte att ett ingripande alltid får positiva konsekvenser för den som äger eller använder informationssystemet. Om myndigheten orsakar skador på systemet eller förstör information

som dess ägare behöver, kan det tvärtom innebära att den som redan utsatts för ett brott drabbas ytterligare. Stiftelsen menar att det inte kan vara rimligt att den som utsatts för ett brott också ska behöva bära kostnaderna och riskerna för myndigheternas försök att ingripa i brottet.

Till detta kommer att konsekvenserna av övervakning och möjligheter till intrång i människors privata sfär inte begränsas till dem som faktiskt utsätts för sådana intrång. Förekomsten av befogenheter att göra intrång påverkar också människors beteenden. Personer som har anledning att värna konfidentialiteten i sina kommunikationer kan komma att avstå från att kommunicera, även när de inte ägnar sig åt något klandervärt. Det kan exempelvis röra sig om personer som utsätts för våld i nära relationer, personer som söker hjälp för psykisk ohälsa eller personer som vill lämna uppgifter om missförhållanden på sin arbetsplats. Dessa kostnader för övervakning har Stiftelsen pekat på i tidigare remissvar. Att den statliga övervakningen i detta fall kallas ”ingripanden i cybermiljö” torde inte påverka dessa kostnader.

Utredaren föreslår vidare i 4 § en särskild befogenhet att tillfälligt bereda sig tillgång till trafikuppgifter under befordran till eller från ett informationssystem. Syftet ska vara att kartlägga om det finns kommunikation med andra informationssystem. Det är således inte fråga om en generell befogenhet att avlyssna innehållet i människors kommunikationer och inte heller om en befogenhet att löpande övervaka all trafik till och från ett informationssystem. Detta innebär emellertid inte att åtgärden saknar betydande integritetskonsekvenser. Uppgifter om vilka informationssystem som kommunicerar med varandra kan ge långtgående information om enskildas aktiviteter, relationer och beteenden, även när innehållet i kommunikationen inte är tillgängligt. Till detta kommer att det kan vara svårt att tekniskt avgränsa vilka trafikuppgifter som berör ett visst informationssystem, i synnerhet i nät där flera användare och tjänster delar på tekniska resurser. En till synes begränsad kartläggning kan därmed komma att beröra även kommunikation som saknar koppling till den verksamhet som myndigheten vill ingripa mot.

Utredningsförslaget innebär risker för säkerheten på internet

Stiftelsen konstaterar att utredaren inte i tillräcklig utsträckning har beaktat hur internet och den digitala infrastruktur som idag används av privatpersoner, företag och myndigheter fungerar. Informationssystem är ofta sammanlänkade och beroende av varandra. En och samma server kan exempelvis användas för att tillhandahålla tjänster till ett stort antal företag och organisationer. Att ett av dessa företag ägnar sig åt brottslig verksamhet innebär inte att det alltid är tekniskt möjligt att ingripa mot den del av serverns funktioner som används för verksamheten utan samtidigt att påverka andra verksamheter.

Liknande problem kan uppstå vid blockering av IP-adresser och domännamn. En IP-adress behöver inte motsvara en viss tjänst eller ens ett visst företag. Ett ingripande som avser att förhindra tillgången till en viss tjänst kan därmed innebära att tillgången till ett stort antal andra tjänster också förhindras. Här bör särskilt de risker som ingripanden i domännamnssystemet (DNS) kan medföra nämnas. Domännamnssystemet utgör en grundläggande del av internets infrastruktur. Ingrepp i denna kan få konsekvenser för verksamheter som inte har någon som helst koppling till den verksamhet som myndigheterna avser att ingripa mot. Utredaren diskuterar förvisso de problem som nedstängning av hela digitala plattformar kan medföra och konstaterar att sådana åtgärder i allmänhet inte kan anses proportionerliga (s. 264f).

Detta löser dock inte problemet med ingripanden som avser en begränsad del av ett informationssystem men som, på grund av hur infrastrukturen fungerar, ändå får omfattande konsekvenser för andra användare och tjänster. Det bör också konstateras här att en kriminell aktör som vill undvika en blockering i många fall har tekniska möjligheter att göra det. En person som är medveten om att myndigheterna försöker ingripa mot en viss tjänst har sannolikt också större incitament än andra användare att vidta liknande åtgärder. Det finns därmed risk för att blockeringar i högre utsträckning kommer att drabba legitim verksamhet än den verksamhet som motiverat blockeringen.

Stiftelsen menar att det, för att kunna avgöra om de föreslagna befogenheterna är proportionerliga, är nödvändigt att beskriva hur de i praktiken skulle användas och vilka konsekvenser de tekniska metoderna skulle få för andra verksamheter. Att lagstiftningen sägs vara teknikneutral innebär inte att utredaren kan bortse från hur tekniken fungerar.

Stiftelsen har i tidigare remissvar pekat på de intressekonflikter som uppstår när svenska myndigheter samtidigt förväntas verka för att skydda svenskarna och svenska företag från dataintrång och själva ska ägna sig åt dataintrång. En viktig del av arbetet med att skydda informationssystem från dataintrång är att identifiera sårbarheter i den programvara och utrustning som används och att se till att dessa sårbarheter åtgärdas.

De myndigheter som ska genomföra dataintrång har emellertid intresse av att sådana sårbarheter inte åtgärdas, eftersom möjligheterna att genomföra intrång i så fall kan försvinna. Utredaren föreslår uttryckligen att myndigheterna ska få bryta mot eller kringgå systemskydd och utnyttja tekniska sårbarheter vid genomförandet av ingripanden. Det innebär att svenska myndigheter ges incitament att bevara kunskap om sårbarheter som skulle kunna användas för att angripa svenska informationssystem. Att en myndighet får kännedom om en sårbarhet och avstår från att informera den som tillhandahåller den aktuella programvaran eller utrustningen innebär dock inte att myndigheten därmed har ensam tillgång till sårbarheten. En sårbarhet som kan användas av svenska brottsbekämpande myndigheter kan också användas av organiserad brottslighet eller av främmande makts underrättelsetjänster. Det finns också en risk att information om de sårbarheter som myndigheterna har kännedom om läcker, exempelvis genom att myndigheterna själva utsätts för dataintrång. Det är därmed inte givet att en utökning av svenska myndigheters möjligheter att genomföra dataintrång skulle leda till att säkerheten i svenska informationssystem ökar. Den kan tvärtom leda till att säkerheten minskar och att möjligheterna för kriminella att begå brott ökar.

Stiftelsen finner det särskilt anmärkningsvärt att utredaren uttryckligen avvisar ett krav motsvarande det som gäller vid hemlig dataavläsning, nämligen att informationssäkerheten efter verkställigheten ska hålla minst samma nivå som när den påbörjades. Utredaren menar bland annat att sådana krav inte lämpar sig för de ingripanden som nu föreslås eftersom syftet med ingripandena kan vara att påverka informations tillgänglighet och riktighet (s. 308f).

Detta resonemang tar emellertid inte tillräcklig hänsyn till skillnaden mellan att ett ingripande avsiktligt påverkar vissa uppgifters tillgänglighet och att ingripandet lämnar kvar tekniska sårbarheter som kan utnyttjas vid framtida dataintrång. Att viss information avsiktligt har blockerats innebär inte att det skulle vara befogat att lämna ett informationssystem med en

lägre säkerhetsnivå än det hade före ingripandet. Stiftelsen menar att utgångspunkten måste vara att svenska myndigheter som får kännedom om sårbarheter i informationssystem ska verka för att dessa åtgärdas, inte för att de ska finnas kvar. I den mån undantag från detta överhuvudtaget ska kunna göras måste beslut om sådana undantag fattas av någon annan än den myndighet som har ett intresse av att sårbarheten inte åtgärdas. Undantagen måste, i den mån de alls ska förekomma, vidare vara tidsbegränsade och föremål för oberoende kontroll. Det måste också ställas krav på att myndigheterna efter ett ingripande återställer informationssystemens säkerhet i den utsträckning detta är möjligt utan att det lagligen beslutade ingripandets syfte omintetgörs.

Till detta kommer att de informationssystem som svenska myndigheter vill ingripa mot kan vara av betydelse för Sveriges egen säkerhet. Ett informationssystem kan exempelvis vara en del av infrastruktur som Försvarsmakten eller andra totalförsvarsaktörer är beroende av, utan att detta är känt för den myndighet som vill ingripa.

Risker med förstörelse av information

En av de befogenheter som utredaren föreslår att myndigheterna ska ges är rätten att radera information. En viktig skillnad mellan denna befogenhet och flera av de övriga befogenheterna som föreslås är att konsekvenserna av att den används i många fall är oåterkalleliga.

Utredaren har uppmärksammat detta och föreslår därför särskilda begränsningar för radering. Enligt 5 § krävs att ingripandet är av synnerlig vikt för att förhindra eller avbryta ett brott. Radering ska vidare användas restriktivt och i regel endast när mindre ingripande åtgärder inte är tillräckliga. Beslut om radering ska som huvudregel fattas av åklagare, även om särskilt utsedda befattningshavare vid de brottsbekämpande myndigheterna i brådskande situationer ska kunna fatta interimistiska beslut (s. 252–258, 263f, 283ff). Stiftelsen menar emellertid att de föreslagna begränsningarna inte är tillräckliga.

Det kan exempelvis konstateras att ett interimistiskt beslut om radering kan ha hunnit genomföras innan åklagaren i efterhand prövar om det fanns grund för beslutet. Om åklagaren då finner att beslutet varit felaktigt är det inte säkert att det finns någon möjlighet att återställa den information som raderats. Utredaren föreslår visserligen att en kopia av uppgifterna, om möjligt, ska bevaras för att underlätta åklagarens prövning och att den enskilde, under vissa förutsättningar, ska kunna få tillgång till en sådan kopia. Att en kopia ska bevaras är dock inte ett absolut krav.

Stiftelsen noterar också att utredaren uttryckligen avvisar en särskild möjlighet att överklaga eller få domstolsprövning av åklagarens beslut om radering. En efterhandskontroll av om det var befogat att förstöra informationen innebär emellertid inte att informationen återställs. Det kan också vara av betydelse för möjligheterna att utreda och lagföra brott om den information som myndigheterna vill förstöra finns kvar. Detsamma gäller för personer som på felaktiga grunder misstänks för brott och som skulle kunna använda informationen för att visa att misstankarna är grundlösa. Utredaren menar att de föreslagna ingripandena inte har som syfte att utreda brott. Samtidigt konstaterar utredaren att information som blir tillgänglig genom ingripandena kan användas i förundersökningar. Att myndigheterna själva inte haft som huvudsakligt syfte att

samla in bevisning innebär således inte att åtgärderna saknar betydelse för möjligheterna att säkra bevisning eller för enskildas rätt till en rättvis rättegång.

Stiftelsen menar att en eventuell befogenhet att förstöra information måste omgärdas av särskilt starka rättssäkerhetsmekanismer och att beslut om radering bör föregås av domstolsprövning.

Problem med företagens medverkansskyldighet

Utredaren föreslår i 20 § att verksamhetsutövare som omfattas av anmälningsplikt enligt 2 kap. 1 § lagen om elektronisk kommunikation (LEK) ska vara skyldiga att medverka vid myndigheternas ingripanden. I den föreslagna förordningen anges att denna medverkan bland annat kan innebära att tillhandahålla teknisk information och använda tillgängliga tekniska metoder. Stiftelsen noterar att utredaren utgår ifrån att medverkansskyldigheten ska begränsas till sådana möjligheter som redan finns tillgängliga för verksamhetsutövaren. Detta är emellertid inte tillräckligt tydligt reglerat i lagförslaget.

Det bör också klargöras att det finns en betydande skillnad mellan företag som tillhandahåller kommunikationstjänster och företag som tillhandahåller de tjänster som användarna kommunicerar med eller via. Att en person använder en viss internetoperatör för att kommunicera med en tjänst innebär inte att internetoperatören har tillgång till eller kan påverka den information som lagras i tjänsten. Inte heller innebär det att operatören har tillgång till innehållet i kommunikationen. Om operatören inte har tillgång till den information som myndigheterna vill komma åt eller tekniska möjligheter att vidta de åtgärder som myndigheterna vill ha vidtagna, kan en medverkansskyldighet endast få avsedd effekt om operatören åläggs att göra förändringar i sina system eller om andra tekniska skydd undanröjs.

Stiftelsen menar att det uttryckligen måste framgå av lagstiftningen att en medverkansskyldighet inte kan innebära en skyldighet att bygga in bakdörrar, försvaga kryptering eller på annat sätt försämra säkerheten för användarna.

Det bör också framgå att medverkan aldrig får innebära att operatören åläggs att behandla uppgifter i strid med andra rättsliga skyldigheter. Här kan särskilt nämnas att företag som tillhandahåller elektroniska kommunikationsnät och kommunikationstjänster redan omfattas av krav på att skydda säkerheten i sina system och användarnas kommunikationer. Att ålägga företag att vidta åtgärder som innebär att de inte längre kan uppfylla dessa skyldigheter framstår som synnerligen ogenomtänkt. Utredaren föreslår att företagen ska få ersättning för kostnader som uppkommer i samband med deras medverkan. Det är en rimlig utgångspunkt. Det är emellertid inte tillräckligt att ersätta de direkta kostnaderna för att lämna uppgifter eller vidta en viss åtgärd. Även kostnader för att hantera säkerhetsrisker, återställa system och ersätta skador som uppstår hos kunder eller andra måste beaktas. Det är inte rimligt att privata företag ska behöva bära det ekonomiska ansvaret för konsekvenserna av ingripanden som beslutats av svenska myndigheter.

Förslaget saknar tillräckliga kontrollmekanismer

Stiftelsen konstaterar att utredaren föreslår att myndigheterna i stor utsträckning själva ska få avgöra när de ska använda de föreslagna befogenheterna. Enligt 11 § ska särskilt utsedda befattningshavare vid Polismyndigheten, Säkerhetspolisen och Tullverket få fatta beslut om ingripanden enligt 3 och 4 §§, liksom om tillträde till annars skyddade platser när detta behövs för ingripandet. Radering ska som huvudregel beslutas av åklagare. Som tidigare nämnts föreslås dock också en möjlighet för myndigheterna att i brådskande situationer fatta interimistiska beslut om radering. Stiftelsen menar att denna beslutsordning inte ger tillräckligt skydd mot godtycke och missbruk. Det måste finnas en reell möjlighet för någon annan än den myndighet som vill vidta en viss åtgärd att bedöma om det finns grund för att vidta den. Detta måste också innebära att det finns en praktisk möjlighet att neka myndigheten att vidta åtgärden.

Att det finns regler om vilka omständigheter som ska föreligga för att en myndighet ska få genomföra ett dataintrång är av begränsat värde om det endast är myndigheten själv som avgör om dessa omständigheter föreligger. Stiftelsen menar att beslut om ingripanden som innebär intrång i människors privata informationssystem, tillgång till trafikuppgifter om deras kommunikationer eller ändring, blockering eller radering av information som huvudregel måste fattas av domstol.

En möjlighet att i verkligt brådskande situationer genomföra en åtgärd innan en sådan prövning har kunnat ske skulle kunna övervägas. En sådan möjlighet måste emellertid vara tydligt begränsad och förenas med en obligatorisk och skyndsam efterhandsprövning samt ett strikt ansvar för uppkomna skador. Det är också nödvändigt att det finns effektiva möjligheter att granska det faktiska genomförandet av de åtgärder som myndigheterna vidtar.

Att en myndighet har fått tillstånd att vidta en viss åtgärd innebär inte att det därmed är visat att de åtgärder som myndigheten faktiskt har vidtagit har omfattats av tillståndet. Detta förutsätter bland annat att de åtgärder som vidtas dokumenteras på ett sådant sätt att det i efterhand går att avgöra vilka informationssystem myndigheten har berett sig tillgång till, vilken information myndigheten har tagit del av, vilka förändringar som har gjorts i systemen och vilka skador som har uppstått. Stiftelsen noterar att utredaren föreslår en dokumentationsskyldighet enligt 23 § samt särskild tillsyn av Säkerhets- och integritetsskyddsnämnden. Det är i sig positivt men inte tillräckligt. Det är också nödvändigt att tillsynen omfattar de ingripanden som myndigheterna betecknar som misslyckade. Att myndigheten inte lyckats uppnå det syfte som den haft med ett ingripande innebär inte att ingripandet inte har inneburit ett intrång i någons privatliv eller orsakat skador på ett informationssystem.

Brister rörande enskildas möjligheter att få kännedom om ingripanden och tillvarata sin rätt

Ett problem som finns i flera av de lagar som ger myndigheter befogenheter att i hemlighet övervaka enskilda är att den som utsatts för olaglig övervakning normalt saknar möjlighet att få reda på att så skett. Det innebär i sin tur att vederbörande saknar praktiska möjligheter att tillvarata sin rätt, exempelvis genom att begära ersättning för det intrång i privatlivet som har skett.

Detta problem blir än större med den lagstiftning som nu föreslås, eftersom de åtgärder som myndigheterna ska få vidta inte enbart innebär tillgång till information, utan också kan innebära att information förstörs eller att informationssystem skadas. Utredaren föreslår i 21 § att enskilda som fått uppgifter raderade eller blockerade under längre tid än en månad, som huvudregel, ska underrättas om ingripandet. Undantag föreslås dock bland annat om personen inte kan identifieras genom rimliga åtgärder eller om viss sekretess gäller. Någon generell skyldighet att underrätta enskilda om andra ingripanden föreslås inte. Utredaren motiverar detta bland annat med att den enskilde ändå ofta kommer att upptäcka ingripandet (s. 317–325.) Detta resonemang är svårt att förstå.

En person som upptäcker att information har försvunnit från dennes dator eller telefon har med den föreslagna lagstiftningen inte nödvändigtvis några möjligheter att få reda på om detta beror på att svenska myndigheter har gjort ett intrång i utrustningen, på att någon annan har gjort ett intrång eller på ett tekniskt fel. Om ett ingripande inte leder till någon synlig förändring av systemets funktioner, kan det dessutom vara helt omöjligt för den enskilde att upptäcka att ett intrång har ägt rum. Detta gäller särskilt vid ingripanden som syftar till att tillfälligt kartlägga trafikuppgifter.

Stiftelsen finner det också anmärkningsvärt att utredaren inte föreslår någon skyldighet för Säkerhets- och integritetsskyddsnämnden att, på begäran av en enskild, kontrollera om det har gjorts ett ingripande enligt den nya lagen och om ingripandet i så fall har varit lagenligt. Utredaren konstaterar uttryckligen att någon sådan skyldighet inte bör införas (s. 338).

Det innebär att enskilda som misstänker att de har utsatts för olagliga ingripanden kommer att sakna rätt till den typ av kontroll som finns i delar av den övriga lagstiftningen om hemliga tvångsmedel. Stiftelsen menar att det inte finns skäl att neka personer eller företag som utsatts för olagliga ingripanden från svenska myndigheter effektiva möjligheter att tillvarata sina rättigheter. Det måste därför finnas en skyldighet att underrätta dem som utsatts för ingripanden så snart som möjligt, utan att syftet med ett i övrigt lagenligt ingripande äventyras.

Eventuella beslut om att inte underrätta den som utsatts måste vara föremål för en oberoende prövning. För att kontrollmekanismerna ska kunna betraktas som effektiva krävs det också att överträdelser av reglerna kan leda till sanktioner för dem som har överträtt dem. Utredaren bedömer att de nuvarande skadeståndsreglerna ger tillräckliga möjligheter till ersättning för den som drabbas av ett felaktigt ingripande. Någon särskild skadeståndsreglering föreslås därför inte (s. 350–354).

Stiftelsen delar inte denna bedömning. Det kan konstateras att ett lagenligt ingripande kan orsaka omfattande skador för personer som inte har någon koppling till den brottslighet som motiverat ingripandet. Om exempelvis ett ingripande mot ett visst informationssystem leder till att en annan verksamhet inte längre kan använda sina informationssystem, kan det orsaka mycket stora ekonomiska skador. Detsamma gäller om information förstörs, om ett system blir otillgängligt eller om en sårbarhet som en myndighet har utnyttjat vid ett ingripande senare utnyttjas av någon annan.

Det är inte rimligt att enskilda eller företag som saknar koppling till brottsligheten ska behöva bära kostnaderna för sådana skador enbart därför att myndighetens beslut i sig har varit lagligt.

Stiftelsen menar därför att staten måste bära det fulla ekonomiska ansvaret för skador som myndigheternas ingripanden orsakar för oskyldiga tredje parter. Det bör också säkerställas att den som utsatts för ett felaktigt ingripande har praktiska möjligheter att få ersättning för såväl ekonomiska skador som integritetsintrång och andra kränkningar av grundläggande fri- och rättigheter. För att dessa möjligheter ska vara effektiva krävs, som tidigare framhållits, att den enskilde också kan få reda på att ingripandet ägt rum.

Frågan om tidsbegränsad lagstiftning och utvärdering

Utredaren föreslår att lagstiftningen ska vara tidsbegränsad till fem år, från den 1 juli 2027 till och med utgången av juni 2032. En utvärdering av lagens behov och nytta förutsätts inför ett eventuellt beslut om att permanenta den. Stiftelsen menar att en tidsbegränsning av lagstiftningen inte kan kompensera för brister i utredningsunderlaget eller för att lagstiftningen inte uppfyller de krav som följer av RF och EKMR. Att människors grundläggande rättigheter endast får kränkas med stöd av en viss lagstiftning under fem år gör inte kränkningarna mer acceptabla.

Erfarenheterna från tidigare lagstiftning inom övervakningsområdet visar också att det finns anledning att vara skeptisk till föreställningen att lagstiftning som ger myndigheter nya befogenheter kommer att sluta gälla när myndigheterna väl har börjat använda dem. Det finns tvärtom en risk att myndigheterna kommer att hänvisa till att befogenheterna har blivit en del av deras normala verksamhet som skäl för att lagstiftningen ska permanentas.

För att en utvärdering överhuvudtaget ska kunna ge svar på om lagstiftningen har varit ändamålsenlig måste det, innan lagstiftningen införs, definieras vad som ska utvärderas och vilka uppgifter som måste samlas in för att detta ska kunna göras. Antalet ingripanden som myndigheterna genomfört eller antalet informationssystem som myndigheterna lyckats göra intrång i kan inte användas som tillräckliga mått på lagstiftningens effektivitet. (När det gäller exempelvis hemlig dataavläsning har utvärderingarna som gjorts visat att majoriteten av ingripandena inte skett mot personer som senare lagförts för brott, det vill säga inte bara har de inte lagförts för de brott som det hemliga tvångsmedlet motiverats med utan inte överhuvudtaget. Detta bör ses som en stark indikation på att de har använts mot personer som inte har begått några brott.) Om syftet med lagstiftningen är att förhindra brott måste det utvärderas i vilken utsträckning brottsligheten faktiskt har minskat som en följd av den. Man måste också kunna visa att sambandet är kausalt, det vill säga att det inte räcker att säga att brottsligheten har minskat.

Till detta måste läggas en utvärdering av de negativa konsekvenserna av lagstiftningen, bland annat antalet felaktiga ingripanden, konsekvenserna för personer som inte har varit misstänkta för brott, skador på informationssystem och konsekvenserna för säkerheten på internet. Stiftelsen menar dock att det, innan en lagstiftning som innebär inskränkningar av människors grundläggande fri- och rättigheter införs, måste kunna visas vara nödvändig och proportionerlig. Det kan inte vara meningen att staten först ska ges befogenheter att göra intrång i människors privatliv och därefter, när intrången redan har skett, utreda om det fanns skäl att ge staten dessa befogenheter.

Om 5 julistiftelsen

5 Julistiftelsen arbetar för mänskliga rättigheter, integritet och säkerhet på internet. 5 Julistiftelsen grundades 2013 av ett antal svenska internetveteraner som ville värna mänskliga rättigheter på internet, enligt den FN-resolution som antogs den 5 juli 2012 och som slog fast att mänskliga rättigheter ska gälla även där.

5 Julistiftelsen tillhandahåller verktyg som hjälper internetanvändare att öka sin frihet, säkerhet och integritet och ägnar sig åt informationsverksamhet och opinionsbildning i dessa frågor.

www.5july.org