Justitiedepartementet
ju.remissvar@regeringskansliet.se
ju.L4@regeringskansliet.se

Stockholm den 2 november 2026

Telenors yttrande över betänkandet Effektiva ingripanden mot brott i cybermiljö, Ju2026/01670

1. Sammanfattning

Telenor Sverige AB (Telenor) delar utredningens bedömning att brott och brottslig verksamhet i cybermiljö utgör ett allvarligt samhällsproblem och att de brottsbekämpande myndigheterna behöver ändamålsenliga verktyg för att kunna förhindra sådan brottslighet. Ett effektivt regelverk kan stärka såväl enskildas trygghet som tilliten till digitala tjänster och elektronisk kommunikation.

Telenor kan emellertid inte tillstyrka utredningens förslag i dess nuvarande utformning. De föreslagna befogenheterna innebär att myndigheter kan bereda sig tillgång till informationssystem, kringgå systemskydd, kartlägga kommunikation, ändra eller blockera uppgifter, radera data och ta sig in på skyddade platser. Åtgärderna kan få stora konsekvenser för privatliv, kommunikationshemlighet, egendomsskydd, informationssäkerhet och driftskontinuitet. Den tänkta beslutsordningen och de föreslagna rättssäkerhetsgarantierna motsvarar enligt Telenors bedömning inte ingreppens potentiella omfattning och allvar.

Telenor anser sammanfattningsvis att ett fortsatt lagstiftningsarbete bör utgå från följande.

Ingripanden som innebär tillgång till eller påverkan på informationssystem och kommunikation ska som huvudregel omfattas av oberoende förhandsprövning.

Ingripanden får inte kunna användas för att kringgå de högre krav på misstankegrad, brottets karaktär och oberoende prövning som gäller för hemliga tvångsmedel eller andra motsvarande straffprocessuella åtgärder.

Medverkansskyldigheten för aktörer som är anmälda enligt lagen om elektronisk kommunikation (LEK) måste avgränsas tydligt till konkreta och individuella beslut och får inte utvecklas till en generell anpassnings- eller beredskapsskyldighet.

Åtgärder ska i första hand riktas mot den aktör eller tekniska resurs som kontrollerar det brottsliga innehållet eller den brottsliga tjänsten, inte mot en operatör som endast förmedlar elektronisk kommunikation.

Beslut måste vara tekniskt avgränsade, riskbedömda, dokumenterade och förenade med klara regler om ansvar, kostnadsersättning och skadestånd.

Transparens, tillsyn och möjlighet till rättslig prövning måste förstärkas.

2. Övergripande synpunkter

2.1 Behovet av effektiva ingripanden

Telenor instämmer i problembeskrivningen och motsätter sig inte att myndigheterna under tydligt angivna förutsättningar ges bättre möjligheter att ingripa mot allvarlig brottslighet i cybermiljö. Telenor motsätter sig inte att handlingar som annars skulle kunna utgöra dataintrång under noggrant angivna förutsättningar ges stöd i lag. Särskilda åtgärder mot digital infrastruktur som uteslutande eller huvudsakligen används för allvarlig brottslighet kan vara motiverade. En sådan reglering måste dock vara proportionerlig och innehålla skyddsmekanismer som är anpassade till åtgärdernas faktiska effekter och inte enbart till hur åtgärderna rubriceras.

2.2 Beredningsunderlaget och konsekvensanalysen

Telenor anser att beredningsunderlaget är otillräckligt när det gäller konsekvenserna för de företag vars nät, system, lokaler och personal kan beröras. LEK-anmälda aktörer har en särställning i förslaget genom den uttryckliga medverkansskyldigheten, men operatörsperspektivet har inte varit tillräckligt representerat under utredningsarbetet. Detta märks särskilt i avsaknaden av en konkret analys av hur ingripanden kan påverka säkerhet, driftskontinuitet, kunders kommunikation, säkerhetsskyddad verksamhet och operatörernas ansvar gentemot kunder och andra berörda tredje parter.

Utredningens kontakter under arbetet förefaller huvudsakligen ha avsett brottsbekämpande myndigheter och andra offentliga aktörer. Leverantörer av elektroniska kommunikationsnät och kommunikationstjänster har däremot inte redovisats som en särskild konsultationsgrupp, trots att dessa aktörer föreslås omfattas av en uttrycklig medverkansskyldighet och kan behöva hantera betydande tekniska, säkerhetsmässiga och avtalsrättsliga konsekvenser. Detta förstärker behovet av kompletterande beredning.

Den fortsatta behandlingen av förslaget bör därför föregås av en fördjupad teknisk och rättslig konsekvensanalys tillsammans med leverantörer av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Analysen bör skilja mellan internetaccess och annan ren överföring å ena sidan och värdtjänster, plattformstjänster och molntjänster å andra sidan, då förutsättningar för ingripanden mot berörda informationssystem skiljer sig väsentligt.

En strukturerad teknisk analys bör innehålla scenariotester för den typ av åtgärder som kan bli aktuella, inkl. blockering, radering, lösenordsändring, utnyttjande av sårbarheter, installation av tekniska hjälpmedel och påverkan på delad infrastruktur. Resultatet bör redovisas öppet i lagstiftningsärendet.

3. Synpunkter på utredningens förslag

3.1 En ny lag och lagens tillämpningsområde (avsnitt 13)

Telenor har förståelse för att en samlad reglering kan ge bättre överblick än spridda bestämmelser. Begreppen ”cybermiljö” och ”informationssystem” är emellertid mycket vidsträckta. De omfattar potentiellt allt från en enskild uppkopplad enhet till centrala nätfunktioner och teknisk infrastruktur som betjänar ett mycket stort antal användare. Detta gör det svårt för marknadsaktörer att förutse vilka system och verksamheter som kan bli föremål för ingripanden.

Lagen bör därför innehålla en tydligare differentiering mellan informationssystem som används av den aktör som bedriver den brottsliga verksamheten, system som tillhör en mellanhand som enbart överför informationen (mere conduit) samt system hos aktörer som utövar kontroll över innehållet. En operatör som endast överför innehållet har normalt varken kontroll över det underliggande innehållet eller rätt att ta del av eller styra kommunikationen. En åtgärd mot sådan infrastruktur kan dessutom påverka ett stort antal användare som saknar koppling till den brottsliga verksamheten. Det är också viktigt att uppmärksamma att slutanvändares enheter som är uppkopplade mot mellanhänders infrastruktur normalt inte kontrolleras eller styrs av mellanhanden.

För att öka proportionaliteten i förslaget bör det också införas en uttrycklig subsidiaritetsregel som går ut på att ingripanden mot en mellanhand eller delad kommunikationsinfrastruktur endast får ske när en åtgärd mot den som kontrollerar innehållet, tjänsten eller den brottsliga resursen inte är möjlig eller skulle vara uppenbart otillräcklig. Skälen för att i stället rikta åtgärden mot mellanhanden ska dokumenteras i beslutet.

3.2 Jurisdiktion för informationssystem i utlandet

Informationssystem och uppgifter i cybermiljö är gränsöverskridande. Ett system som framstår som tillgängligt från Sverige kan vara distribuerat över flera länder, och den faktiska lagringsplatsen kan vara okänd eller förändras under pågående verkställighet.

Att aktivt ändra, blockera eller radera uppgifter innebär en faktisk påverkan på ett informationssystem och ingreppet kan utgöra utövning av jurisdiktion på en annan stats territorium. En anknytning till Sverige grundar inte i sig rätt att vidta en sådan åtgärd i utlandet. Utredningen tar inte tillräcklig höjd för denna aspekt.

3.3 Ändamålen med ingripandena och kravet på särskild vikt (avsnitt 14.1–14.4)

De föreslagna ändamålen är breda och kan tillämpas redan när det antas att ett informationssystem utnyttjas i brottslig verksamhet. Detta kombineras med ett strafftröskelkrav på endast ett års fängelse i straffskalan och att någon identifierad misstänkt inte behöver finnas. Tillämpningsområdet blir därmed potentiellt omfattande.

Telenor anser att förutsättningarna måste preciseras så att ingripanden inte kan grundas på allmänna antaganden om ett system, en tjänst eller en

användarkategori. Det ska krävas konkret och verifierbar information om kopplingen mellan det avgränsade informationssystemet och den aktuella brottsligheten samt om varför den valda åtgärden förväntas få avsedd effekt.

För ingripanden som kan ge myndigheten tillgång till trafikuppgifter under befordran eller påverka tredje mans kommunikation gäller att det inte får bildas ett snabbspår som alternativ till hemlig övervakning eller avlyssning, och det bör för dessa fall krävas brottslighet av högre svårhetsgrad än den generella ettårs-tröskeln. Helst bör lagen innehålla en uttömmande brottskatalog för sådana särskilt ingripande åtgärder.

3.4 Tillgång till informationssystem, blockering och andra liknande åtgärder (avsnitt 14.2–14.3)

Befogenheten att bereda sig tillgång till informationssystem och därefter ändra eller blockera uppgifter eller vidta ”annan liknande åtgärd” är svår att överblicka. Teknikneutral reglering är ofta eftersträvansvärd, men den får inte bli så öppen att det saknas förutsebara gränser för vilka handlingar som är tillåtna. Detta gäller särskilt när systemskydd får kringgås och tekniska sårbarheter utnyttjas.

Åtgärder som påverkar elektronisk kommunikation eller teknisk infrastruktur kan potentiellt få spridningseffekter långt utanför den tilltänkta måltavlan. En blockering, lösenordsändring eller aktiv störning kan påverka legitim trafik, alarmering, samhällsviktiga tjänster och företagskunders verksamhet. Att medvetet störa ett informationssystems funktion utan föregående teknisk samordning med den som driver eller kontrollerar systemet kan medföra skadeverkningar som från ett drifts- och säkerhetsperspektiv är jämförbara med ett obehörigt angrepp. Det gäller särskilt i delade, driftskritiska eller säkerhetskänsliga miljöer. Generella formuleringar om aktsamhet är inte tillräckliga för att hantera dessa risker.

Begreppet ”annan liknande åtgärd” bör antingen tas bort eller kompletteras med en tydlig yttre gräns i lag. Sådana andra åtgärder måste vara funktionellt jämförbara med de uttryckligen angivna åtgärderna och får inte innebära större integritets-, säkerhets- eller driftsrelaterade risker än de i lagen uppräknade.

3.5 Radering (avsnitt 14.5 och 16.2)

Radering är i regel oåterkallelig och kan medföra betydande skada för enskilda, företag och för datas värde som bevisning. Telenor delar bedömningen att kraven för beslut om radering måste vara högre än för andra åtgärder men menar att en åklagarprövning inte utgör en tillräckligt oberoende kontroll. Ingrepp av denna känsliga natur bör godkännas av domstol efter ansökan av åklagare.

Möjligheten till interimistiska beslut avsedda för sällsynta fall kan lätt i praktiken överutnyttjas och bör därför begränsas till klart definierade nödsituationer där det föreligger en högst konkret och omedelbar risk för allvarlig skada och där mindre ingripande åtgärder, såsom blockering eller isolering, inte kan användas. Interimistiskt beslut bör underställas domstol utan dröjsmål. Det bör också finnas en faktisk möjlighet till rättslig prövning och gottgörelse när radering har varit felaktig.

Om radering genomförs kan det argumenteras för att en verifierbar kopia eller annan tillräcklig teknisk dokumentation som huvudregel ska säkras före

åtgärden, om detta kan ske utan att den risk som motiverar raderingen förverkligas. Hanteringen av kopian ska omfattas av tydliga regler om åtkomst, användningsbegränsning, bevarande och förstöring.

3.6 Proportionalitet och skydd för tredje man (avsnitt 14.6–14.8)

Telenor välkomnar att proportionalitetsprincipen uttrycks i lagen. Den föreslagna bestämmelsen behöver dock kompletteras för miljöer där många användare delar nät, adresser, servrar eller andra resurser. Det räcker inte att väga intrånget för den vars uppgifter direkt omfattas av ingripandet. Bedömningen måste även omfatta påverkan på övriga användare, informationssäkerhet, nät- och driftsäkerhet, samhällsviktiga tjänster samt risken för att åtgärden skapar eller blottlägger sårbarheter.

Beslutet bör innehålla en särskild tredjemans- och systemriskbedömning. Ett ingripande i delad infrastruktur bör inte få genomföras om det finns en beaktansvärd risk för omfattande störningar, förlust av konfidentialitet eller påverkan på samhällsviktig verksamhet, annat än vid omedelbar fara för liv, hälsa eller rikets säkerhet och efter oberoende prövning.

3.7 Vem som bör besluta om ingripanden (avsnitt 16)

Telenor avstyrker att merparten av ingripandena ska kunna beslutas internt av särskilt utsedda befattningshavare vid den verkställande myndigheten. Åtgärdernas karaktär, snarare än deras beteckning som ”polisiära ingripanden”, bör avgöra kontrollnivån. När myndigheten i hemlighet kan kringgå skydd, få tillgång till trafikuppgifter och kommunikation, ändra uppgifter eller påverka ett informationssystems funktion finns uppenbara likheter med hemliga och preventiva tvångsmedel.

Som huvudregel bör beslut fattas av domstol efter ansökan av åklagare. En skyndsam jourordning kan ge nödvändig operativ snabbhet. I akuta situationer kan ett interimistiskt myndighetsbeslut accepteras endast om det underställs domstol inom en kort och lagbestämd frist och om åtgärden omedelbart upphör när den inte godkänns. Det interimistiska förfarandet får inte i praktiken bli det vanligaste tillvägagångssättet.

Lagen kan som ett gångbart alternativ i stället ange vilka kategorier av mindre ingripande och fullt reversibla åtgärder som undantagsvis får beslutas internt. Alla åtgärder som innebär åtkomst till kommunikation under befordran, utnyttjande av tekniska sårbarheter, hemligt tillträde, påverkan på delad infrastruktur eller risk för betydande tredjemansskada bör däremot omfattas av oberoende förhandsprövning på samma sätt som gäller för beslut om hemliga tvångsmedel.

Telenor noterar att utredningens egen internationella jämförelse visar att beslut om motsvarande åtgärder i de flesta undersökta länder fattas av domstol, åklagare eller undersökningsdomare. Den svenska beslutsmodell som föreslås framstår därför inte som en nödvändig följd av åtgärdernas digitala karaktär. Tvärtom talar jämförelsen för att operativ snabbhet kan förenas med oberoende förhandsprövning och snabba interimistiska förfaranden. Ett interimistiskt beslut bör underställas domstol senast inom 24 timmar efter det att verkställigheten inleddes.

3.8 Beslutens innehåll och villkor (avsnitt 17.1–17.2)

Telenor tillstyrker att beslut som huvudregel ska vara skriftliga och ange ändamål, brottslighet, informationssystem, åtgärd, tidsram och villkor. För en medverkande operatör behöver beslutet vara tillräckligt preciserat för att det ska gå att avgöra vad som rättsligt och tekniskt sett krävs samt vilka system och användare som får påverkas.

Beslutet bör därför alltid, inte endast ”om möjligt”, ange vilken avgränsad del av informationssystemet som omfattas. Om en sådan avgränsning inte kan göras bör beslutet särskilt motivera detta och redovisa hur påverkan på legitim verksamhet ska begränsas.

Beslutet bör vidare i relevanta fall innehålla en bedömning av svensk jurisdiktion och när delad infrastruktur berörs, ett högsta tillåtet skade- eller påverkansområde. Beslutet ska ange vilka användare, systemdelar, trafikslag och tekniska beroenden som inte får påverkas.

Om ingripandet kan medföra behandling av trafikuppgifter eller kommunikation under befordran ska beslutet uttryckligen ange vilka uppgiftskategorier som får behandlas, för vilket ändamål, under vilken tid samt när och hur uppgifterna ska förstöras eller återställas.

När en LEK-anmäld aktör ska medverka bör beslutet också ange kontaktpunkt, ansvarig beslutsfattare, teknisk genomförandeplan, tillåtna metoder, riskbegränsande villkor, loggningskrav, kostnadsansvar, sekretessförutsättningar och ett förfarande för omedelbar eskalering om operatören bedömer att verkställigheten medför allvarlig säkerhets- eller driftsrisk.

Telenor kan som utgångspunkt inte acceptera att för bolaget helt okända tekniska metoder används för att kringgå vårt fysiska och logiska skydd mot intrång, skadegörelse och sabotage. Det gäller för hemliga tvångsmedel och det gäller även om nu aktuellt förslag skulle bli verklighet.

3.9 Tillträde till platser (avsnitt 17.3)

Möjligheten att i hemlighet bereda sig tillträde till platser för att installera tekniska hjälpmedel är synnerligen ingripande. För teleoperatörer kan berörda platser vara driftskritiska, säkerhetsskyddade och är genomgående föremål för strikta åtkomst- och arbetsmiljöregler. Oannonserat tillträde kan i sig skapa incidenter och innebära risk för personal, utrustning och tjänster.

Beslut om tillträde till driftskritiska eller säkerhetskänsliga lokaler bör därför alltid föregås av oberoende prövning och innehålla särskilda villkor. Huvudregeln bör vara att tillträde samordnas med utsedda säkerhetsprövade kontaktpersoner hos verksamhetsutövaren, om inte domstol uttryckligen bedömer att detta skulle omintetgöra ändamålet.

Lagen bör innehålla ett uttryckligt förbud mot att genomföra installation eller annan åtgärd på ett sätt som åsidosätter säkerhetsskydd, fysisk säkerhet, elsäkerhet eller driftsäkerhetsrutiner. Den verkställande myndigheten bör bära ett tydligt ansvar för att anlitad personal har dokumenterad teknisk kompetens för den aktuella miljön.

3.10 Metoder för genomförande och aktsamhetskrav (avsnitt 18.2–18.3)

Telenor motsätter sig inte att en laglig befogenhet måste kunna verkställas effektivt. Befogenheten att bryta eller kringgå systemskydd och utnyttja tekniska sårbarheter kräver emellertid betydligt mer detaljerade skyddsregler. En använd sårbarhet kan kvarstå efter ingripandet, upptäckas av andra aktörer eller påverka systemets säkerhet för legitima användare.

Aktsamhetskravet bör därför kompletteras med krav på dokumenterad riskanalys före verkställighet, löpande skadebegränsning, fullständig teknisk loggning, återställande samt underrättelse till systemägaren om sårbarheter och förändringar när sekretesskäl inte längre hindrar detta.

Det kan vara lämpligt att införa en skyldighet att genomföra en efterkontroll tillsammans med berörd verksamhetsutövare när en åtgärd har påverkat operatörens system eller lokaler. Kontrollen bör säkerställa att installerade hjälpmedel har avlägsnats, att behörigheter och konfigurationer har återställts och att nya sårbarheter inte har uppstått.

3.11 Medverkansskyldighet för LEK-anmälda aktörer (avsnitt 18.4)

Telenor avstyrker den föreslagna medverkansskyldigheten i dess nuvarande, generellt hållna form. Skyldigheten riktas mot aktörer som bedriver verksamhet som ska anmälas enligt LEK, trots att dessa aktörer ofta endast förmedlar kommunikation och saknar kontroll och inflytande över det brottsliga innehållet, den aktuella plattformen eller den nätverksanslutna enheten.

Medverkansskyldigheten måste därtill strikt skiljas från en skyldighet att i förväg anpassa nät, system, organisation eller beredskap. Erfarenheterna av medverkansskyldigheten vid hemlig dataavläsning visar enligt Telenor att otydliga regler kan leda till krav som i praktiken innebär generell teknisk anpassning inför framtida, ännu inte beslutade verkställigheter. En sådan problematisk utveckling får inte upprepas.

Lagen bör därför uttryckligen ange att medverkan endast får avse tillgängliga uppgifter, funktioner och tekniska metoder inom ramen för ett konkret och giltigt beslut. Skyldigheten får inte innebära krav på utveckling, anskaffning eller permanent installation av ny funktionalitet, försvagning av säkerhetsfunktioner eller skapande av generell åtkomst till nät och system. Medverkan ska vidare alltid vara knuten till ett aktivt beslut om åtgärder och kravet på medverkan ska således aldrig kunna göras gällande i syfte att förbereda eller effektivisera eventuella framtida beslut om åtgärder. Att ställa upp sådana krav utgör inte medverkan, utan innefattar anpassning.

Operatören måste också ha rätt att invända mot eller begära skyndsam omprövning av en verkställighetsbegäran som går utanför beslutet, är tekniskt ogenomförbar eller medför en oacceptabel risk för säkerhet, drift eller tredje man. En sådan invändning bör ha inhiberande verkan, utom möjligtvis vid en konkret och omedelbar fara där en oberoende beslutsfattare har godkänt fortsatt verkställighet.

Medverkansskyldigheten bör därtill begränsas av en uttrycklig ”kontrollprincip”: en aktör kan endast åläggas att göra det som ligger inom aktörens faktiska tekniska och rättsliga kontroll. Operatören ska exempelvis aldrig behöva ta

ansvar för innehåll, plattformar, slutenheter eller krypteringslösningar som den inte utövar kontroll eller inflytande över.

Telenor noterar att även PTS framhåller att det måste vara möjligt att förutse om en medverkansskyldighet föreligger, formerna för medverkan och skyldighetens gränser samt att medverkan endast bör omfatta information som redan finns tillgänglig hos operatören. Detta talar för att begränsningen ska framgå direkt av lag och inte endast av motivuttalanden eller förordning.

En begäran om medverkan får inte heller innebära att operatören ska behandla trafikuppgifter, innehåll eller andra uppgifter på ett sätt som annars är förbjudet enligt LEK eller tillämplig dataskyddsreglering, om inte undantaget har ett tydligt och preciserat stöd i lag. Det måste särskilt klargöras hur en begäran om ändring eller radering förhåller sig till operatörens skyldigheter att bevara trafikuppgifter, säkra spårbarhet och rapportera säkerhetsincidenter.

Regeringen föreslås få meddela närmare föreskrifter om medverkans-skyldighetens innebörd. Sådana föreskrifter får inte utformas så att medverkan kan tolkas som en skyldighet att vidta generella eller förberedande anpassningsåtgärder. Telenor har erfarenhet av att 3§ 3 och 4 förordningen (2020:64) om hemlig dataavläsning har åberopats på ett sätt som enligt Telenors uppfattning riskerar att sudda ut gränsen mellan medverkan i ett enskilt fall och generell teknisk anpassning. Den nya regleringen bör därför innehålla en uttrycklig avgränsning på lagnivå. Motsvarande tydlig avgränsning bör övervägas även i regelverket om hemlig dataavläsning.

3.12 Kostnader, ansvar och skadestånd

Telenor tillstyrker att en medverkande aktör ska ha rätt till ersättning, men regleringen behöver preciseras. Ersättningen bör omfatta samtliga skäliga och verifierbara merkostnader som har ett direkt orsakssamband med beslutet eller verkställigheten, inklusive intern och extern personal, beredskap utanför ordinarie arbetstid, säkerhetsåtgärder, tekniska tester, återställande, incidenthantering samt kostnader för att hantera kund- och tredjemansanspråk. Ersättning bör även kunna lämnas för dokumenterad undanträngning av ordinarie verksamhet när denna varit en nödvändig följd av en skyndsam medverkansbegäran.

Det ska särskilt beaktas att medverkan kräver omedelbar uppmärksamhet och således tar i anspråk personella resurser som normalt redan är upptagna av ordinarie arbetsuppgifter och att det därför kan uppstå betydande olägenheter i verksamheten som inte enbart kan mätas i pengar.

Det måste också klargöras vem som bär ansvaret om en myndighetsåtgärd orsakar driftavbrott, dataförlust, säkerhetsincident, avtalsbrott gentemot kund eller annan tredjemansskada. En operatör som lojalt medverkar enligt ett myndighetsbeslut bör inte bära civilrättsligt eller offentligrättsligt ansvar för följder som orsakas av den beslutade eller anvisade åtgärden.

Staten bör ta på sig ett primärt och strikt ansvar för skador som orsakas genom ett ingripande eller en medverkansbegäran, om inte skadan beror på att den medverkande aktören uppsåtligen eller genom grov vårdslöshet har avvikit från beslutet. Det bör även finnas ett snabbt ersättningsförfarande för drabbade

tredje parter och verksamhetsutövare. En ansökan om ersättning bör avgöras inom en bestämd tid och beslutet bör kunna överklagas.

3.13 Underrättelse, dokumentation, tillsyn och rättsmedel (avsnitt 19)

Telenor tillstyrker förslagen om dokumentation och särskild tillsyn men vill återigen betona att de inte kompenserar för avsaknaden av oberoende förhandskontroll för åtgärder som i sak är lika ingripande som hemliga tvångsmedel. En efterhandsgranskning kan konstatera fel, men kan inte återställa raderade uppgifter eller reparera ett intrång i kommunikationshemligheten, en allvarlig driftsstörning eller uppkomst av sårbarheter eller andra negativa följdverkningar.

Underrättelseskyldigheten bör vara bredare och omfatta den som äger eller driver ett informationssystem när denne har berörts av ett hemligt ingripande, så snart sekretesskäl inte längre hindrar sådan underrättelse. Underrättelsen bör innehålla tillräcklig information för att den som berörs ska kunna bedöma ingripandets laglighet och vid behov utnyttja ett effektivt rättsmedel.

Det bör finnas en generell möjlighet till domstolsprövning av beslut och verkställighetsåtgärder, åtminstone i efterhand. För pågående blockering eller annan fortlöpande påverkan måste det finnas möjlighet till skyndsam prövning och interimistiskt upphävande.

En LEK-anmäld aktör som har ålagts att medverka bör ha rätt att få själva medverkansbeslutet och dess omfattning prövade, även om aktören inte är den som ingripandet ytterst riktar sig mot. Prövningen måste omfatta om begäran ryms inom beslutet, om den är proportionerlig och om den innebär otillåten anpassning eller oacceptabla säkerhets- och driftsrisker.

Tillsynsmyndigheten bör få löpande tillgång till samtliga beslut och tekniska verkställighetsprotokoll, inte endast underrättas i vissa fall av felaktig interimistisk radering. Detta gör sig särskilt gällande under den femåriga begränsade tid som regelverket står under särskild utvärdering. Tillsynen bör årligen redovisa aggregerad statistik över åtgärdstyper, beslutsnivåer, ingripanden mot delad infrastruktur, inträffade skador och konstaterade brister. Utan sådan insyn i tillämpningen blir det svårare att utvärdera huruvida ingripandemöjligheten ska avskaffas, förlängas eller göras permanent.

3.14 Tidsbegränsning och utvärdering (avsnitt 19.4)

Telenor tillstyrker att lagen tidsbegränsas. En femårig giltighetstid innebär dock inte att åtgärderna i sak är mer proportionerliga. För att riksdagen ska kunna ta ställning till regleringens framtid måste en oberoende utvärdering planeras från början och baseras på dokumenterade uppgifter om effektivitet, integritetsintrång, driftsrisker, kostnader, tredjemanspåverkan och rättsliga invändningar.

Utvärderingen bör inte begränsas till antalet genomförda ingripanden eller till om myndigheterna tekniskt har lyckats blockera, ändra eller radera uppgifter. Den bör mäta om ingripandena har lett till en varaktig minskning av den aktuella brottsligheten, om verksamheten har flyttats till annan infrastruktur eller jurisdiktion och om samma resultat hade kunnat uppnås genom mindre ingripande åtgärder.

En eventuell förlängning eller permanentning bör kräva ett nytt aktivt ställningstagande av riksdagen på grundval av en oberoende utvärdering. Lagen bör upphöra automatiskt om ett sådant beslut inte fattas före giltighetstidens utgång.

4. Avslutande synpunkter

Telenor ser i likhet med regeringen ett behov av att säkerställa samhällets förmåga att ingripa mot allvarlig brottslighet i cybermiljö. För att reglering på området ska vara långsiktigt hållbar måste den vara förutsebar, proportionerlig och förenad med kontrollmekanismer som motsvarar befogenheternas faktiska ingripande karaktär.

Telenor anser att det lämnade förslaget inte är vederbörligt utrett i flera aspekter och att det därför bör omarbetas innan det läggs till grund för lagstiftning. Det fortsatta arbetet bör särskilt inriktas på oberoende förhandsprövning, större förståelse för de olika aktörerna i värdekedjan, en högre grad av precision i tillämpningsområdet, ett starkare skydd för tredje man och påverkad infrastruktur, en strikt avgränsning mellan medverkan och anpassning samt tydliga regler om teknisk riskhantering, ansvar, ersättning och effektiva rättsmedel.

Telenor står till Justitiedepartementets förfogande för fortsatt dialog om hur ett effektivt och rättssäkert regelverk kan utformas med beaktande av de tekniska, säkerhetsmässiga och rättsliga förutsättningarna för tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

Telenor Sverige AB

Martin Sjöberg
Bolagsjurist