Effektiva ingripanden mot brott i cybermiljö

Delbetänkande av Utredningen om hemliga och preventiva tvångsmedel

Stockholm 2026

STATENS OFFENTLIGA UTREDNINGAR

SOU 2026:45

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Multiply Solutions
Tryck och remisshantering: Multiply Solutions, Stockholm 2026

ISBN 978-91-525-1573-0 (tryck)
ISBN 978-91-525-1574-7 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Den 20 februari 2025 beslutade regeringen att tillkalla en särskild utredare med uppdraget att göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel i syfte att åstadkomma en mer effektiv och tydlig reglering och att förbättra möjligheterna att använda tvångsmedlen i brottsbekämpningens olika faser (dir. 2025:12). Samma dag förordnades Gunnel Lindberg, dåvarande ordförande i Säkerhets- och integritetsskyddsnämnden, till särskild utredare. Utredningen har antagit namnet Utredningen om hemliga och preventiva tvångsmedel.

Den 28 april 2025 förordnades kanslirådet i Justitiedepartementet Sophie Blomgren och den 12 maj 2025 departementssekreteraren i Försvarsdepartementet Magnus Calais att vara sakkunniga i utredningen. Den 28 april 2025 förordnades som experter i utredningen chefsrådmannen Axel Peterson, Sveriges domstolar, byråchefen Eva Bloch, Åklagarmyndigheten, vice överåklagaren Ted Murelius, Ekobrottsmyndigheten, verksjuristen Karolina Helling och enhetschefen Robert Nygren, Säkerhetspolisen, juristerna Matilda Svahn och Steffen Oxenvad, Polismyndigheten, enhetschefen Ida Olsson, Myndigheten för säkerhet och integritetsskydd, verksjuristen Micaela Nordberg, Tullverket, avdelningsjuristen Andreas Persson, Integritetskyddsmyndigheten, och advokaten Bengt Ivarsson, Sveriges advokatsamfund. Den 12 september 2025 entledigades Magnus Calais och i hans ställe förordnades den 19 september 2025 ämnessakkunnige Tomas Borg, Försvarsdepartementet. Som sekreterare i utredningen anställdes den 24 februari 2025 rättssakkunniga i Justitiedepartementet Anna Ziesnitz, den 17 mars 2025 numera hovrättsrådet Emelie Hansell och den 1 maj 2025 rådmannen Malin Stensbäck. Den 29 maj 2026 entledigades Emelie Hansell. Rådman-

nen Anna Hempel anställdes den 1 juni 2026. Hon har dock inte deltagit i arbetet med delbetänkandet.

Utredningen har i arbetet kunnat beakta lagstiftning och andra förhållanden fram till den 1 juni 2026. Utredningen överlämnar härmed delbetänkandet Effektiva ingripanden mot brott i cybermiljö, SOU 2026:45. Återstående frågor kommer att behandlas i slutbetänkandet.

Stockholm i juni 2026

Gunnel Lindberg

Emelie Hansell
Malin Stensbäck
Anna Ziesnitz

Innehåll

Bilagor

Sammanfattning

Uppdraget

Enligt direktiven har den ökade digitaliseringen och den tekniska utvecklingen öppnat nya möjligheter för kriminalitet. Kriminella aktörer använder i allt större utsträckning avancerad teknologi för att begå brott. Det handlar inte enbart om brott som begås digitalt, utan nästan alla brott har i dag en digital komponent. Brott och brottslig verksamhet i cybermiljö utgör därmed ett växande hot mot både enskilda och den nationella säkerheten.

Utvecklingen har lett till att de brottsbekämpande myndigheterna i dag inte har tillräckligt effektiva verktyg för att bekämpa sådan brottslighet. Det finns ett behov av att ändra strategi till att i större utsträckning aktivt förhindra, störa och avbryta brott och brottslig verksamhet i cybermiljö. Utredningens uppdrag har mot den bakgrunden varit bl.a. att kartlägga andra jämförbara länders rättsliga möjligheter, analysera behovet av åtgärder för att förhindra, störa och avbryta brott och brottslig verksamhet i cybermiljö och lämna nödvändiga författningsförslag.

Bakgrunden till förslagen

Det moderna samhället präglas av att informationsteknik genomsyrar i stort sett alla sektorer. Internet har skapat nya möjligheter att snabbt och enkelt få tillgång till och kunna distribuera information, men digitaliseringen medför samtidigt nya sårbarheter som kan utnyttjas av kriminella och främmande makt. I takt med att samhället har digitaliserats har även kriminaliteten flyttat in i den digitala miljön. Brott kan begås utan att gärningsmannen är fysiskt på plats, samtidigt som kryptering och anonymiseringsverktyg gör det svårt

att knyta en person till brott som begås med hjälp av digitala informationssystem. Cyberbrott utgör både ett generellt samhällshot och ett hot mot enskilda. Myndigheterna har särskilt framhållit att de inte kan fullgöra sina uppdrag med dagens lagstiftning.

Den digitala miljön saknar, i motsats till den fysiska, tydliga gränser. Det innebär att det ofta är oklart var brott begås och var bevisning finns. Den nuvarande lagstiftningen är i allt väsentligt anpassad till den fysiska miljön och processrättsliga åtgärder är främst inriktade på att utreda och lagföra brott. Det innebär enligt utredningens mening att de rättsliga förutsättningarna som de brottsbekämpande myndigheterna har inte är tillräckliga för att hantera dagens brottslighet i cybermiljö.

Ett centralt hinder är att de åtgärder som behöver vidtas för att ingripa i digital miljö – bl.a. att bereda sig tillgång till informationssystem, att ändra eller blockera uppgifter i systemen eller att radera uppgifter – typiskt sett omfattas av straffbestämmelsen om dataintrång. Den nuvarande regleringen ger inte de brottsbekämpande myndigheterna rätt att vidta sådana åtgärder.

Det finns därmed ett tydligt behov av att stärka de brottsbekämpande myndigheternas möjligheter att ingripa mot brott i cybermiljö, särskilt genom åtgärder som kan vidtas i ett tidigare skede och som möjliggör att brottslig verksamhet kan förhindras, störas eller avbrytas.

En ny lag om ingripanden i cybermiljö

En ny lag är det bästa alternativet

Utredningen föreslår att det ska införas en ny lag om ingripanden i cybermiljö, benämnd lagen om polisiära ingripanden i cybermiljö. Regleringen bedöms inte lämpligen kunna inordnas i befintlig lagstiftning. Lagen ska framför allt tillämpas av Polismyndigheten och Säkerhetspolisen men även av Tullverket.

Möjligheten att ingripa bör gälla i cybermiljö

Lagens tillämpningsområde ska avgränsas till cybermiljö. Med cybermiljö avses den digitala miljö där information skapas, bearbetas, lagras och kommuniceras genom sammankopplade informationssystem. Begreppet omfattar bl.a. internet, sociala medier, digitala plattformar och teknisk infrastruktur som servrar, nätverk och lagringstjänster. Begreppet informationssystem ska också användas för att avgränsa lagens tillämpningsområde. Informationssystem omfattar hårdvara, mjukvara, databaser och nätverkskomponenter som används för att automatiskt behandla digital information.

Möjligheten att ingripa måste enligt utredningens mening fungera både på underrättelsestadiet och på utredningsstadiet. Regleringen ska därför vara tillämplig såväl för att förhindra och avbryta brott som för att störa och avbryta brottslig verksamhet.

Cybermiljön innebär särskilda utmaningar för den internationella rättsordningen, eftersom brottsligheten ofta bedrivs över nationsgränser. Gärningsman, brottsoffer, servrar och data kan befinna sig i olika länder samtidigt som uppgifter snabbt kan flyttas mellan olika jurisdiktioner. Den nya lagen måste utformas med hänsyn till folkrättens principer och regleringen om svensk domstols behörighet i brottmål. Tillämpningsområdet behöver begränsas, eftersom cybermiljön saknar traditionella gränser. Det görs genom att lagen bara ska vara tillämplig om det finns tydlig anknytning till Sverige.

Anknytningen till svenska förhållanden

Utredningen föreslår att lagen ska vara tillämplig på brott som begås eller kommer att begås i cybermiljö med hjälp av informationssystem om

- brottet begås av någon som befinner sig i Sverige,
- brottet riktas mot någon eller något i Sverige, eller
- informationssystemet finns i Sverige.

Anknytningsfaktorerna är alternativa, vilket innebär att det är tillräckligt att en av dem är uppfylld för att lagen ska kunna tillämpas. Det innebär vidare att ingripanden kan göras även om gärningsman-

nen befinner sig utomlands, så länge brottet riktas mot svenska intressen eller begås med hjälp av informationssystem som finns i Sverige.

Närmare om ändamålen med ingripandena

Ändamålen med ingripandena måste framgå tydligt av lagen för att säkerställa rättssäkerhet och begränsa tillämpningsområdet. Ett ingripande ska endast få göras för de ändamål som anges i lagen och det ska finnas faktiska omständigheter som visar att syftet med ingripandet kan uppnås.

Utredningen föreslår att ingripanden får beslutas om det är av särskild vikt för att

- förhindra eller avbryta brott i cybermiljö,
- störa eller avbryta brottslig verksamhet i cybermiljö, eller
- kartlägga om ett informationssystem utnyttjas i brottslig verksamhet i cybermiljö.

Ett centralt ändamål för ingripanden är att förhindra konkreta brott innan de begås. Ingripanden ska därför kunna göras redan på underrättelsestadiet när det finns objektiva omständigheter som stödjer bedömningen att brott kommer att begås. Ingripanden ska även kunna göras för att avbryta pågående brott. Exempel på situationer där tidiga ingripanden kan behövas är

- systematiska bedrägerier,
- spridning av skadlig programvara,
- försäljning av narkotika och andra illegala varor via internet,
- ransomwareangrepp,
- digital rekrytering till allvarlig brottslighet, och
- cyberspionage och förberedelse till terroristbrott.

Ett annat viktigt ändamål för ingripande är att störa eller avbryta brottslig verksamhet även om det ännu inte går att identifiera konkreta brott.

Ingripanden för att störa eller avbryta brottslig verksamhet kan exempelvis bestå i att

- blockera tillgång till webbplatser,
- begränsa tillgången till uppgifter som används för brott, och
- förhindra spridning av läckta personuppgifter eller kontokortsuppgifter.

Ett ytterligare ändamål för ingripande är att kartlägga digital infrastruktur som antas utnyttjas i brottslig verksamhet. Genom att tillfälligt bereda sig tillgång till trafikuppgifter under befordran till eller från ett informationssystem, kan myndigheterna kartlägga om ett informationssystem, som antas utnyttjas i brottslig verksamhet i cybermiljö, kommunicerar med andra informationssystem. Genom att kartlägga sådan infrastruktur kan myndigheterna mer effektivt ingripa mot den brottsliga verksamheten.

Krav för att få ingripa

Utredningen föreslår att ingripanden av nämnda slag i cybermiljö endast får göras om det är av särskild vikt för det aktuella ändamålet. Bedömningen ska bygga på konkreta omständigheter och får inte grundas på spekulationer eller allmänna antaganden. Kravet på särskild vikt innebär både att ingripandet ska förväntas få betydelse för brottsbekämpningen och att det ska finnas ett tydligt behov av ingripande i det enskilda fallet.

Vad befogenheterna innebär

De brottsbekämpande myndigheterna föreslås få rätt att bereda sig tillgång till informationssystem och uppgifter i sådana system utan att göra sig skyldiga till dataintrång. Att en myndighet bereder sig tillgång till informationssystem är normalt en förutsättning för att den ska kunna ingripa på det sätt som är syftet med den nya lagen, men inte ett absolut krav i alla situationer.

Myndigheterna föreslås vidare få rätt att ändra uppgifter som ger tillgång till informationssystem, exempelvis genom att byta lösenord och tillfälligt ta över tillgången till ett informationssystem. De andra

åtgärder som får vidtas är att blockera uppgifter som ger tillgång till eller behandlas i informationssystem. Myndigheterna får också genom någon annan liknande åtgärd störa eller hindra användningen av uppgifter som behandlas i informationssystem.

Endast kortvariga åtgärder tillåts. Den som berörs av ett ingripande ska senare kunna återfå rådigheten över informationssystemet eller uppgifterna.

Särskilt om radering

Radering innebär att uppgifter helt eller delvis förstörs. Myndigheterna förslås i vissa fall få radera uppgifter, exempelvis övergreppsmaterial eller skadlig programvara. Radering skiljer sig från blockering genom att åtgärden är oåterkallelig, vilket anses innebära större risk för skada och integritetsintrång.

Radering ska enligt förslaget därför få användas endast när mindre ingripande åtgärder inte är tillräckliga och när det är nödvändigt för att förhindra eller avbryta brott i cybermiljö, exempelvis terrorism, spionerі eller barnpornografibrott. Det ställs också högre krav för beslut om radering än för andra typer av ingripanden. Beslut om radering får endast fattas om ingripandet är av synnerlig vikt för att förhindra eller avbryta brott i cybermiljö. Det ska alltså vara mycket svårt eller omöjligt att uppnå samma resultat genom andra, mindre ingripande, åtgärder.

Krav som ska gälla för alla typer av ingripanden

Varje åtgärd enligt den nya lagen ska ha en tydlig koppling till ändamålet med ingripandet. Ingripanden får endast riktas mot uppgifter i de delar av informationssystemet som har samband med brott eller brottslig verksamhet av tillräcklig svårhetsgrad och för de särskilt angivna ändamålen.

Ingripanden får endast beslutas vid brott eller brottslig verksamhet som innefattar brott med minst ett års fängelse i straffskalan och som begås eller kommer att begås i cybermiljö med hjälp av informationssystem.

Alla ingripanden ska vara proportionerliga. Ingripandets art, styrka, räckvidd och varaktighet ska alltså stå i rimlig proportion till syf-

tet. Beslutsfattaren måste först pröva om ingripandet är tillåtet, därefter om det är nödvändigt och slutligen om det är proportionerligt. I första hand ska den minst ingripande åtgärden användas.

Vid bedömningen ska hänsyn tas till hur allvarlig brottsligheten är, vilken skada den kan orsaka och hur stort integritetsintrång åtgärden medför.

Förbud mot ingripanden

Utredningen föreslår särskilda skyddsregler för vissa informationssystem och uppgifter. Ingripanden får inte riktas mot informationssystem som stadigvarande används för journalistisk verksamhet där det råder grundlagsskyddad tystnadsplikt eller verksamhet för bikt och själavård inom trossamfund.

Ingripanden får inte heller avse uppgifter som omfattas av tystnadsplikt enligt reglerna om undantag från vittnesplikt enligt vissa bestämmelser i rättegångsbalken, exempelvis uppgifter som anförtrotts advokater, läkare, psykologer eller försvarare i deras yrkesutövning.

Om det, när ett ingripande genomförs, upptäcks att skyddade uppgifter eller informationssystem berörs, ska ingripandet omedelbart avbrytas och eventuell information som omfattas av förbud förstöras.

Vem som får fatta beslut enligt lagen

Ingripanden enligt lagen liknar mer andra typer av polisiära ingripanden än åtgärder som kräver beslut av domstol eller åklagare. Befattningshavare vid Polismyndigheten, Säkerhetspolisen och Tullverket ska därför enligt förslaget få besluta om de flesta typer av ingripanden enligt lagen. För att säkerställa rättssäkerheten ska besluten fattas av särskilt utsedda befattningshavare vid myndigheterna med tillräcklig kompetens. Kompetenskraven regleras i förordning (bl.a. krav på särskild kunskap om digitala informationssystem och om informationssäkerhet).

Beslut om radering, som är en oåterkallelig åtgärd och som får anses medföra större integritetsintrång än andra ingripanden i cyber-

miljö, ska däremot fattas av åklagare efter ansökan från Polismyndigheten, Säkerhetspolisen eller Tullverket.

Om det kan befaras att det skulle uppstå en fördröjning av väsentlig betydelse för ändamålet med ingripandet att invänta åklagares beslut, ska tidigare nämnda, särskilt utsedda befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket i undantagsfall kunna fatta interimistiskt beslut om radering. Det kan t.ex. vara fråga om radering av terrorisminnehåll, säkerhetskänslig information eller skadlig kod, där ett omedelbart ingripande krävs för att skydda liv, hälsa eller rikets säkerhet. Interimistiska beslut får endast avse ingripanden mot pågående eller omedelbart förestående brott och möjligheten att fatta sådana beslut bör användas restriktivt. Ett interimistiskt beslut ska så snart som möjligt anmälas skriftligen till åklagare tillsammans med motiveringen för ingripandet. Om möjligt ska en kopia av de raderade uppgifterna bifogas, för att åklagaren ska kunna bedöma lagligheten av åtgärden. Om det inte är tekniskt eller praktiskt möjligt, ska uppgifterna dokumenteras på annat sätt. Åklagaren ska så snart som möjligt pröva om det finns grund för beslutet och upphäva det om sådan grund saknas.

Innehållet i besluten

Beslut om ingripanden enligt den nya lagen ska som huvudregel vara skriftliga. I brådskande situationer ska ett muntligt beslut få fattas men det ska därefter dokumenteras så snart det är möjligt. Beslut ska innehålla all information som behövs för att ingripandet ska kunna genomföras. Det innebär att besluten bl.a. ska ange ändamålet med ingripandet, vilket brott eller vilken brottslig verksamhet som ingripandet avser, vilket informationssystem som omfattas, vilka åtgärder som får vidtas, eventuella villkor och om beslut om tillträde har fattats. Vidare ska det anges vilken tidsram som gäller för att genomföra ingripandet, eftersom ingripanden i cybermiljö ofta är beroende av tekniska möjligheter och därför kräver flexibilitet i fråga om genomförandet. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad från beslutet.

Beslutsfattaren ska alltid överväga om ett beslut om ingripande bör förenas med särskilda villkor för att skydda enskildas personliga integritet. Villkor kan t.ex. begränsa vilka delar av ett informations-

system som får granskas eller hur ingripandet får genomföras. Behovet av villkor är särskilt stort när ett informationssystem innehåller stora mängder integritetskänsliga uppgifter eller används av flera personer.

Verkställighet

Omedelbar verkställighet och särskilda aktsamhetskrav

Utredningen föreslår att beslut enligt lagen får verkställas omedelbart, om inte annat anges. När ingripandet genomförs får de tekniska hjälpmedel som behövs användas. Myndigheterna får bryta eller kringgå systemskydd och utnyttja tekniska sårbarheter för att bereda sig tillgång till informationssystem. Det kan göras både genom avancerade tekniska åtgärder och genom enklare metoder, som inloggning med användarnamn och lösenord eller byte av lösenord.

Särskilda aktsamhetskrav ska gälla. Ingripandena ska genomföras så att olägenhet eller skada inte orsakas utöver vad som är absolut nödvändigt. Påverkan på andra användare av samma informationssystem ska begränsas så långt som det är möjligt.

Om tekniska hjälpmedel har installerats ska de tas bort eller göras obrukbara så snart ingripandet har genomförts eller beslutet om ingripande har upphört att gälla.

Utredningen föreslår att den som bedriver viss verksamhet som ska anmälas enligt lagen om elektronisk kommunikation ska vara skyldig att på begäran medverka vid genomförandet av ingripanden enligt den nya lagen. Den som medverkar ska ha rätt till ersättning för de kostnader som uppstår.

Beslut om tillträde

För att genomföra ingripanden ska beslut kunna fattas om tillträde till platser som annars inte är allmänt tillgängliga för att kunna installera tekniska hjälpmedel. Det krävs särskild anledning att anta att informationssystemet finns på den plats som beslutet om tillträde avser. För stadigvarande bostäder krävs synnerlig anledning, vilket innebär ett mycket högt beviskrav.

Beslut om tillträde får inte avse lokaler som används för journalistisk verksamhet, advokatverksamhet, sjukvård, psykologisk verksamhet eller själavård och bikt, eftersom sådana miljöer regelmässigt innehåller mycket integritetskänslig information och därför bör ha ett starkare skydd.

När tillstånd ska upphävas

Utredningen föreslår att ett beslut om ingripande ska upphävas så snart det inte längre finns skäl för det. Enskilda ska inte utsättas för integritetsintrång längre än nödvändigt och i cybermiljö kan förhållandena förändras snabbt. Ett beslut bör därför upphävas när ingripandet har genomförts eller när förutsättningarna för ingripandet har fallit bort. Den ingripande myndigheten – Polismyndigheten, Säkerhetspolisen eller Tullverket – ansvarar för att löpande pröva om det fortfarande finns behov av ingripandet.

Rättssäkerhetsgarantier

Underrättelse till enskilda

Underrättelser om ingripanden kan utgöra en viktig rättssäkerhetsgaranti. Det finns dock inte något generellt behov av underrättelser till enskilda om ingripanden enligt lagen. Det beror dels på att ingripandena ofta äger rum helt öppet, dels på att det ofta är okänt vem som ska underrättas.

Enligt förslaget ska en enskild vars uppgifter har raderats eller blockerats under längre tid än en månad underrättas om ingripandet så snart det lämpligen kan ske. Det gäller dock bara om personen inte redan har fått kännedom om ingripandet. Underrättelse får underlåtas om det inte är känt vem som ska underrättas och personen inte heller genom rimliga åtgärder kan identifieras. Underrättelse får också underlåtas om det råder viss sekretess.

Underrättelse till Säkerhets- och integritetsskyddsnämnden

Enligt förslaget ska åklagaren underrätta Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd om ett interimistiskt beslut om radering genomförts innan åklagaren hunnit pröva frågan och åklagaren anser att skäl för radering saknas. Bakgrunden är att radering ibland måste genomföras mycket snabbt, för att förhindra eller avbryta allvarlig brottslighet. I sådana situationer är det viktigt med möjlighet till tillsyn.

Dokumentation

Både beslut och andra åtgärder enligt den nya lagen ska dokumenteras. Dokumentationsskyldigheten motiveras av rättssäkerhetsskäl och underlättar efterhandskontroll. Dokumentation är central för att säkerställa god förvaltning, motverka godtycklig maktutövning och skapa möjligheter till efterhandskontroll. Dokumentationen syftar till att göra det möjligt att följa hur ingripanden i cybermiljö har genomförts.

Tillsyn

Den nya lagstiftningen kräver särskild tillsyn, mot bakgrund av riskerna för den personliga integriteten. Även om ingripandena ofta sker öppet är det inte säkert att den vars uppgifter har varit föremål för ett ingripande förstår att en brottsbekämpande myndighet har agerat. Den extraordinära tillsyn som utövas av JO och Justitiekanslern samt myndigheternas interna kontroll är därför enligt utredningens mening inte tillräcklig.

Utredningen föreslår att Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd ska utöva tillsyn över tillämpningen av den nya lagen. Tillsynen ska avse frågan om ingripanden görs i enlighet med lag och annan författning.

Den nya lagen och befintlig lagstiftning

I ett särskilt avsnitt går utredningen igenom hur den nya lagstiftningen förhåller sig till befintliga regelsystem för underrättelseverk-

samhet och brottsutredning. Några författningsändringar bedöms inte krävas. Vidare diskuterar utredningen ingående vilket intrång i den personliga integriteten som ingripanden enligt lagen kan innebära och hur de balanseras genom olika rättssäkerhetsåtgärder.

En tidsbegränsad lag som bör träda i kraft snabbt

Den nya lagen föreslås vara tidsbegränsad och gälla i fem år. Det finns ett stort behov av nya verktyg mot cyberbrottslighet, men det är samtidigt svårt att bedöma lagstiftningens effektivitet, praktiska värde och konsekvenser för den personliga integriteten innan den har varit i kraft en tid.

Ändringarna föreslås träda i kraft den 1 juli 2027 och gälla till och med utgången av juni 2032.

Utredningen finner inte behov av några övergångsbestämmelser.

Summary

Remit

As outlined in the inquiry's terms of reference, increased digitalisation and technological developments have opened up new opportunities for criminal activities. Criminal actors increasingly use advanced technologies to commit offences. This does not apply only to offences that are committed digitally; almost all offences committed today have a digital component. Offences and criminal activities in the cyber environment thus pose a growing threat both to individuals and to national security.

As a result of these developments, law enforcement authorities today do not have sufficiently effective tools to combat these kinds of criminal activities. A shift in strategy is needed to ensure that offences and criminal activities in the cyber environment can be prevented, disrupted and stopped to a greater extent. The inquiry was thus tasked with mapping the legal options available in other, comparable countries, analysing the need for measures to prevent, disrupt and stop offences and criminal activities in cyber environment, and making any necessary legislative proposals.

Background to the proposals

In modern society, information technology permeates more or less all sectors. The internet has created new opportunities to quickly and easily access and distribute information, but digitalisation has also brought with it new vulnerabilities that can be exploited by criminals and foreign powers. As society has become digitalised, criminal activities have also moved into the digital environment. Offences can be committed without the perpetrator being physically present,

while encryption and anonymisation tools make it difficult to link an individual to an offence committed using digital information systems. Cyber crime is a threat to both society at large and individuals. The authorities have emphasized that they are unable to carry out their duties under the current legislation.

Unlike the physical environment, the digital environment lacks clear boundaries. This means that it is often unclear where an offence has been committed and where the evidence is. Current legislation is essentially tailored to the physical environment, and procedural law measures primarily focus on investigating and prosecuting offences. In the inquiry's view, this means that the legal conditions under which law enforcement authorities are operating are not sufficient to tackle modern criminal activities in the cyber environment.

One of the primary obstacles is the fact that the necessary measures so as to intervene in a digital environment – including accessing information systems, changing or blocking data in such systems, or deleting data – typically fall under the criminal provision on breach of data security. Current regulations do not allow law enforcement authorities to take such measures.

There is thus a clear need to reinforce the possibilities for law enforcement authorities to intervene in offences in the cyber environment, particularly via measures that can be taken at an early stage and through which criminal activities can be prevented, disrupted or stopped.

A new act on interventions in the cyber environment

A new act is the best option

The inquiry proposes the introduction of a new act on police interventions in the cyber environment. The inquiry has found that these regulations cannot be appropriately incorporated into existing legislation. The act would primarily be applied by the Swedish Police Authority and the Swedish Security Service, but also by Swedish Customs.

Intervention should be possible in the cyber environment

The scope of application of the new act should be limited to the cyber environment. The 'cyber environment' means the digital environment in which data is created, processed, stored and communicated via connected information systems. The term encompasses the internet, social media, digital platforms and technical infrastructure such as servers, networks and storage services. The term 'information systems' should also be used when defining the scope of application of the act. Information systems encompass hardware, software, databases and network components used to automatically process digital information.

Intervention must, in the inquiry's view, be possible at both the intelligence-gathering stage and the investigation stage. The regulations should therefore be applicable both to preventing and stopping offences and to disrupting and stopping criminal activities.

The cyber environment poses particular challenges to the international legal order, as criminal activities are often conducted across national borders. Perpetrators, victims, servers and data may be located in different countries, and data can be moved quickly between jurisdictions.

The new act must be drafted taking account of the principles of international law and the regulations on court jurisdiction of Swedish courts in criminal cases. The scope of application must be limited, since the cyber environment lacks boundaries in the traditional sense. This would be achieved by limiting the application of the act to cases with a clear link to Sweden.

Link to Sweden

The inquiry proposes that the act be applicable to offences that are or will be committed in the cyber environment using information systems where:

- the offence is committed by someone who is in Sweden;
- the offence is directed at someone or something in Sweden; or
- the information system is located in Sweden.

The linking factors are alternative, meaning that the act would be applicable if just one of them is met. This also means that intervention would be possible even if the perpetrator is in another country, as long as the offence is directed at Swedish interests or is committed using information systems located in Sweden.

The purpose of interventions

The purpose of interventions must be clearly stated in the act so as to ensure due process and limit the scope of application. Interventions should only be permitted for the purposes stated in the act, and there must be actual circumstances showing that the purpose of the intervention can be achieved.

The inquiry proposes that an intervention may be ordered if it is of particular importance in order to:

- prevent or stop offences in the cyber environment;
- disrupt or stop criminal activities in the cyber environment; or
- identify whether an information system is being exploited in criminal activities in the cyber environment.

A key purpose of interventions is to prevent specific offences before they are committed. For this reason, it should be possible to intervene as early as the intelligence-gathering stage, as long as there are objective circumstances supporting the assessment that an offence will be committed. It must also be possible to intervene in order to stop an ongoing offence. Situations where early interventions may be necessary include:

- systematic fraud
- dissemination of malware
- sale of narcotics and other illegal goods online
- ransomware attacks
- digital recruitment for serious criminal activities
- cyber espionage and preparatory acts for terrorist offences.

Another important purpose of interventions is to disrupt or stop criminal activities even where specific offences cannot yet be identified.

Interventions to disrupt or stop criminal activities could include:

- blocking access to websites
- restrict access to data used for offences
- prevent the dissemination of leaked personal data or account details.

Another purpose of interventions is identifying digital infrastructure that is likely to be exploited for criminal activities. By temporarily accessing traffic data transmitted to or from an information system, the authorities can identify whether a system that is likely to be exploited for criminal activities in the cyber environment is communicating with other information systems. Identifying such infrastructures would enable the authorities to intervene more effectively against such criminal activities.

Requirements before intervention is permitted

The inquiry proposes that interventions in the cyber environment of the sort outlined above only be permitted if it is of particular importance for the relevant purpose. This must be determined based on concrete circumstances, not on speculation or general assumptions. The 'particular importance' requirement implies that the intervention is expected to be significant in law enforcement terms, and that there is a clear need for intervention in the specific case.

Implications of these powers

It is proposed that the law enforcement authorities be entitled to access information systems and data in those systems without committing the offence of breach of data security. Accessing information systems is usually a prerequisite for a law enforcement authority to be able to intervene in the manner that is the aim of the new act, but it is not an absolute requirement in all situations.

It is also proposed that the authorities be entitled to change data that allows access to information systems, for example by changing passwords or temporarily taking control of access to an information system. The other measures that may be taken are blocking data that provides access to or is processed in the information system. The authorities would also be able to use other, similar measures to disrupt or prevent the use of data processed in the information system.

Only short-term measures would be permitted. Anyone affected by an intervention should later be able to regain control over the information system or data.

Erasure

Erasure means the whole or partial destruction of data. It is proposed that in certain cases, the authorities should be permitted to delete data, e.g. material showing abuse, or malware. Erasure differs from blocking in that it is an irrevocable measure, which is considered to imply a greater risk of damage and breach of privacy.

Under the inquiry's proposal, erasure should thus only be permitted where less intrusive measures are not sufficient, and where it is necessary to prevent or stop offences in the cyber environment, such as terrorism, espionage or child pornography offences. Decisions to order erasure of data will also be subject to higher standards than other types of intervention. Decisions to erase data would only be possible if the intervention is of particular importance to prevent or stop an offence in the cyber environment. This means that it must be very difficult or impossible to achieve the same result through other, less intrusive measures.

Requirements applicable to all types of intervention

Any measure under the new act would have to be clearly linked to the purpose of the intervention. Interventions must only target data in those parts of the information system that are linked to sufficiently serious offences or criminal activities, and for the specifically stated purpose.

Interventions may only be ordered for offences or criminal activities encompassing offences punishable by at least one year's imprisonment and that are or would be committed in the cyber environment using information systems.

All interventions must be proportionate. The nature, strength, reach and duration of the intervention must thus be proportionate to the purpose. The decision-maker must first examine whether the intervention is permitted, then whether it is necessary, and finally whether it is proportionate. The least intrusive measure possible must be employed in the first instance.

When making this assessment, account must be taken of the seriousness of the offence and the damage it could cause, and the magnitude of the breach of privacy entailed by the intervention.

When intervention should not be permitted

The inquiry proposes special protective regulations for certain information systems and data. Interventions should not be allowed to target information systems that are consistently used for journalistic activities, where a constitutionally protected duty of confidentiality applies, or confessional or pastoral care activities within religious communities.

Likewise, interventions should not be permitted to concern data that is subject to confidentiality under the regulations on exemptions from the obligation to give evidence under certain provisions in the Swedish Code of Judicial Procedure, e.g. data confided in lawyers, doctors, psychologists or defence counsels acting in a professional capacity.

If, when an intervention is undertaken, it is discovered that protected data or information systems are involved, the intervention must immediately be discontinued and any information that is not permitted be destroyed.

Decision-makers under the new act

Interventions under the new act would more closely resemble other kinds of police intervention than measures requiring a decision by a court or prosecutor. Under the inquiry's proposal, officials at the

Swedish Police Authority, the Swedish Security Service and Swedish Customs would thus be able to take decisions on most types of interventions under the act. To ensure due process, decisions would have to be taken be specially appointed officials within those authorities, with sufficient expertise. The expertise requirements (e.g. requirement of specific knowledge of digital information systems and information security) would be regulated in an ordinance.

However, decisions on the erasure of data – which is an irrevocable measure and must be considered to entail a greater breach of privacy than other measures in the cyber environment – would be taken by a prosecutor, upon application by the Swedish Police Authority, the Swedish Security Service or Swedish Customs.

If it can be anticipated that awaiting the decision of a prosecutor would lead to a delay of significant effect in terms of the purpose of the intervention, it would be possible in exceptional cases for the aforementioned specially appointed officials at the Swedish Police Authority, the Swedish Security Service or Swedish Customs to take an interim decision on the erasure of data. This could mean, for example, erasing terrorist content, security-sensitive data or malware in cases where immediate intervention is necessary to protect lives, health or national security. Interim decisions should only be possible on interventions in ongoing or imminent offences, and the possibility to take such decisions must be used restrictively. Interim decisions should be notified as soon as possible in writing to a prosecutor, along with the reason for the intervention. If possible, a copy of the erased data should be attached, to enable the prosecutor to assess the legality of the measure. If this is not technically or practically possible, the data should be documented in some other way. The prosecutor must examine as quickly as possible whether there is a legal basis for the decision and cancel the decision if there is no basis for it.

Content of decisions

Decisions on interventions under the new act should, as a rule, be in writing. In urgent situations, an oral decision may be taken but must then be documented as soon as possible. The decision must contain all information that is required for the intervention to be implemen-

ted. This means that decisions must state the purpose of the intervention, the offence or criminal activities targeted by the intervention, the information system concerned, the measures that may be taken, any conditions, and whether a decision has been taken on access. They must also state the applicable time period for implementing the intervention, since interventions in the cyber environment often depend on technical possibilities and thus require flexibility in their implementation. The time period must not be longer than necessary, and no longer than one month from the date of the decision.

The decision-maker must always consider whether a decision on an intervention should be subject to specific conditions so as to protect personal privacy. Conditions could, for example, limit which parts of an information system can be examined or how the intervention can be implemented. There is a particular need for conditions where an information system contains large quantities of privacy-sensitive data or is used by a number of people.

Enforcement

Immediate enforcement and special duty of care

The inquiry proposes that it be possible to enforce decisions under the new act immediately, unless otherwise provided. When an intervention is implemented, the necessary technological tools may be used. The authorities may breach or circumvent system protections and exploit technical vulnerabilities to access information systems. This can be done using both advanced technological measures and simpler methods, such as logging in with a username and password or changing a password.

A special duty of care should apply. Interventions must not be implemented in such a way as to cause inconvenience or damage beyond what is absolutely necessary. Effects on other users of the same information system must be limited as far as possible.

If technological tools have been installed, these must be removed or deactivated as soon as the intervention has been implemented or the decision on intervention has ceased to apply.

The inquiry proposes any operator of an activity who must be notified under the Electronic Communications Act should be obli-

ged to cooperate in the implementation of interventions under the new act. The cooperating operator should be entitled to compensation for any costs that arise.

Decisions on access

For interventions to be implemented, decisions must be taken on access to locations that are otherwise not publicly accessible, so as to install technological tools. Particular grounds to assume that the information system is in the location specified in the decision on access is required. Exceptional grounds – a much higher standard of proof – are required for permanent residential dwellings.

Decisions on access must not concern premises used for journalistic activities, lawyers' activities, medical care, psychological activities or pastoral care or confessions, as such environments routinely contain highly privacy-sensitive information and should therefore be afforded greater protection.

Cancellation of decisions

The inquiry proposes that a decision on intervention should be cancelled as soon as there are no longer any grounds for it. Individuals should not be subjected to breaches of their privacy for longer than is necessary, and in the cyber environment, circumstances can change rapidly. A decision should therefore be cancelled when the intervention has been implemented or when the conditions for the intervention no longer remain. The intervening authority – the Swedish Police Authority, the Swedish Security Service or Swedish Customs – is responsible for continuously ensuring that the intervention is still necessary.

Procedural safeguards

Notifications to individuals

Notifications of interventions can be an important procedural safeguard. However, there is no general need to notify individuals of interventions under the new act. This is because interventions often

take place entirely openly, and also because it is often not known who should be notified.

Under the inquiry's proposal, any individual whose data has been erased or blocked for longer than one month should be notified of the intervention as soon as is reasonably possible. However, this only applies if the person has not already become aware of the intervention. Notification can be waived if it is not known who should be notified and there are no reasonable measures that would enable the person to be identified. Notification can also be waived in certain secrecy circumstances.

Notification of the Commission for Oversight of Privacy Protection in Law Enforcement

Under the inquiry's proposal, a prosecutor must notify the Commission for Oversight of Privacy Protection in Law Enforcement at the Agency for Oversight of Privacy Protection in Law Enforcement when an interim decision on erasure of data has been implemented before the matter could be examined by the prosecutor and the prosecutor has rejected the decision. Data must sometimes be erased very quickly so as to prevent or stop serious criminal activities. In such situations, it is important that supervision can be exercised.

Documentation

Decisions and other measures under the new act must all be documented. This obligation is necessary in view of due process and to facilitate subsequent scrutiny. Documentation is crucial in ensuring good governance, countering arbitrary exercise of power and enabling subsequent scrutiny. The aim of the documentation is to make it possible to trace the implementation of interventions in the cyber environment.

Supervision

In view of the risks to personal privacy, the new legislation requires special supervision. Although interventions will often take place openly, it is not certain that the person whose data has been subject of an intervention will understand that a law enforcement authority has acted. In the inquiry's view, this means that the extraordinary supervision exercised by the Parliamentary Ombudsman and the Office of the Chancellor of Justice and the authorities' own internal controls are not sufficient.

The inquiry proposes that the Commission for Oversight of Privacy Protection in Law Enforcement at the Agency for Oversight of Privacy Protection in Law Enforcement supervise the application of the new act. This supervision should consist in ensuring that interventions are undertaken in accordance with the act and other legislation.

The new act and existing legislation

In a separate section, the inquiry looks at how the new legislation relates to existing regulations for intelligence-gathering and criminal investigations. No legislative amendments are deemed necessary. Furthermore, the inquiry examines in depth the intrusion into personal privacy that interventions under the new act may entail, and how these are counterbalanced by various procedural measures.

A temporary act that should enter into force without delay

It is proposed that the new act be temporary and apply for five years. There is a huge need for new tools to combat cyber crime, but it is also difficult to assess the effectiveness, practical value and personal privacy implications of the legislation until it has been in force for a period.

It is proposed that the amendments enter into force on 1 July 2027 and apply until the end of June 2032.

In the inquiry's estimation, no transitional provisions are required.

1 Författningsförslag

1.1 Förslag till lag (2027:000) om polisiära ingripanden i cybermiljö

Härigenom föreskrivs följande.

Lagens innehåll

1 § Denna lag innehåller bestämmelser om Polismyndighetens, Säkerhetspolisens och Tullverkets befogenheter att ingripa mot brott och brottslig verksamhet i cybermiljö.

Lagens tillämpningsområde

2 § Lagen är endast tillämplig på brott som begås eller kommer att begås i cybermiljö med hjälp av informationssystem, eller på brottslig verksamhet som innefattar sådant brott, om

1. brottet begås av någon som befinner sig i Sverige,
2. brottet riktas mot någon eller något som befinner sig i Sverige, eller
3. informationssystemet finns i Sverige.

Förutsättningarna för ingripanden

3 § Om det är av särskild vikt för att förhindra eller avbryta brott eller störa eller avbryta brottslig verksamhet i cybermiljö, får Polismyndigheten, Säkerhetspolisen eller Tullverket, om det behövs, bereda sig tillgång till ett informationssystem och till uppgifter i det i syfte att

1. ändra eller blockera uppgifter som ger tillgång till eller behandlas i informationssystemet, eller
2. genom en annan liknande åtgärd störa eller hindra användningen av uppgifter som behandlas i informationssystemet.

4 § Om det kan antas att ett informationssystem utnyttjas i brott eller brottslig verksamhet i cybermiljö, får Polismyndigheten, Säkerhetspolisen eller Tullverket tillfälligt bereda sig tillgång till trafikuppgifter under befordran till eller från informationssystemet, om det är av särskild vikt för att kunna kartlägga om det i den brottsliga verksamheten förekommer kommunikation med andra informationssystem.

5 § Om det är av synnerlig vikt för att förhindra eller avbryta brott i cybermiljö får Polismyndigheten, Säkerhetspolisen eller Tullverket radera uppgifter som behandlas i ett informationssystem som myndigheten berett sig tillgång till enligt denna lag.

6 § Ett ingripande enligt 3, 4 eller 5 § får endast avse brott för vilket det är föreskrivet fängelse i ett år eller mer som begås eller kommer att begås i cybermiljö med hjälp av informationssystem, eller brottslig verksamhet som innefattar sådant brott.

Proportionalitet

7 § Ett ingripande enligt denna lag får göras endast om skälen för ingripandet uppväger det intrång eller men i övrigt som det innebär för den vars uppgifter blir föremål för ingripande eller för något annat motstående intresse.

Förbud mot att ingripa

8 § Ett ingripande enligt denna lag får inte avse ett informationssystem som stadigvarande används eller är särskilt avsett att användas i verksamhet

1. där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller

2. för bikt eller enskild själavård som bedrivs av präster inom trossamfund, eller av dem som har motsvarande ställning inom sådana samfund.

Ett ingripande får inte heller avse sådana uppgifter i ett informationssystem som någon, på grund av bestämmelser i 36 kap. 5 § andra och tredje styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om.

Om den ingripande myndigheten får kännedom om att det är fråga om sådana informationssystem som avses i första stycket eller sådana uppgifter som avses i andra stycket ska ingripandet omedelbart avbrytas i den del som det omfattas av förbud. Eventuell information som myndigheten har fått tillgång till och som omfattas av förbud ska förstöras omedelbart.

Beslut om tillträde

9 § Om det är nödvändigt för att ingripa enligt denna lag får den ingripande myndigheten, efter ett särskilt beslut om tillträde, i hemlighet bereda sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång.

Ett beslut enligt första stycket får endast avse en plats där det finns särskild anledning att anta att informationssystemet finns tillgängligt. Om platsen är någons stadigvarande bostad, får ett sådant beslut fattas endast om det finns synnerlig anledning att anta att informationssystemet finns tillgängligt där.

10 § Ett beslut om tillträde enligt 9 § får inte avse en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet

1. där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,

2. som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2025:400) eller av rättegångsombud, deras biträden och försvarare som inte är advokater, eller

3. som bedrivs av präster inom trossamfund, eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Beslut om ingripanden

11 § En särskilt utsedd befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket får besluta om ingripanden enligt 3 och 4 §§. Han eller hon får då även besluta om tillträde enligt 9 §.

12 § En åklagare får, på ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket, besluta om radering enligt 5 §. Han eller hon får då även besluta om tillträde enligt 9 §.

13 § Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för möjligheterna att förhindra förestående brott eller avbryta pågående brott i cybermiljö att inhämta åklagarens beslut, får en särskilt utsedd befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket besluta om radering enligt 5 §. Han eller hon får då även besluta om tillträde enligt 9 §.

Ett beslut enligt första stycket ska så snart som möjligt anmälas till åklagare. Anmälan ska vara skriftlig och innehålla skälen för beslutet. Om möjligt ska en kopia av de uppgifter som har raderats eller ska raderas fogas till anmälan.

14 § Åklagaren ska så snart som möjligt pröva om det finns skäl för ett beslut enligt 13 §. Om åklagaren bedömer att sådana skäl saknas, ska han eller hon omedelbart upphäva beslutet.

Har uppgifterna redan raderats ska åklagaren, i stället för att upphäva beslutet, underrätta Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd om beslutet och sitt ställningstagande. Åklagaren ska då även underrätta den vars uppgifter har raderats, om han eller hon är känd, om sitt ställningstagande och, i förekommande fall, om att han eller hon kan begära hos den ingripande myndigheten att få en kopia av det som har raderats.

Åklagaren ska säkerställa att kopior av raderade uppgifter förstörs senast sex månader efter prövningen.

Villkor

15 § I ett beslut om ingripande enligt denna lag ska det, när det finns skäl för detta, anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

Innehållet i beslut

16 § Ett beslut om ingripande enligt denna lag ska vara skriftligt. Om det skulle medföra en fördröjning av väsentlig betydelse för syftet med ingripandet, får beslutet om ingripande fattas muntligen. Beslutet ska då dokumenteras så snart som möjligt och innehålla de uppgifter som anges i andra stycket.

I beslutet ska följande anges:

1. ändamålet med ingripandet,
2. vilket brott eller vilken brottslig verksamhet som ingripandet avser,
3. vilket informationssystem och, om möjligt, vilken avgränsad del av informationssystemet som ingripandet avser,
4. vilken åtgärd som ingripandet omfattar,
5. när ingripandet senast ska genomföras,
6. de villkor som gäller för ingripandet, och
7. om ett beslut om tillträde enligt 9 § har fattats och vilken plats det i sådana fall omfattar.

Tiden enligt punkten 5 får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet.

Hur ingripanden ska genomföras

17 § Ett beslut om ingripande enligt denna lag får verkställas omedelbart, om inte annat anges.

Vid ingripandet får de tekniska hjälpmedel som behövs användas. Systemskydd får brytas eller kringgås och tekniska sårbarheter får utnyttjas.

18 § Vid ingripandet får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Ingripandet ska genomföras på sådant sätt att påverkan på andra delar av informationssystemet eller

för annan som använder samma del av informationssystemet blir så begränsad som möjligt.

19 § Om ett tekniskt hjälpmedel har installerats, ska hjälpmedlet tas bort eller göras obrukbart så snart som möjligt efter att ingripandet genomförts eller beslutet om ingripande har upphört att gälla.

Skyldighet att medverka

20 § Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation är på begäran av den ingripande myndigheten skyldig att medverka vid ingripanden enligt denna lag.

Den som medverkar enligt första stycket har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den ingripande myndigheten.

Underrättelse till enskild

21 § En enskild, vars uppgifter genom ett ingripande enligt lagen har raderats eller blockerats under längre tid än en månad, ska underrättas om ingripandet så snart det lämpligen kan göras, om inte han eller hon har fått kännedom om ingripandet på annat sätt. Om det inte är känt vem som ska underrättas om ingripandet, och det inte heller finns anledning att anta att denne genom rimliga åtgärder kan identifieras, får underrättelse underlåtas. Underrättelse får också underlåtas om det föreligger sekretess enligt 18 kap. 9 § offentlighets- och sekretesslagen (2009:400).

Den myndighet som har beslutat om ett ingripande som anges i första stycket eller, i fråga om åklagares beslut om radering, har ansökt om radering, ansvarar för underrättelsen. Underrättelse behöver inte lämnas om 14 § andra stycket andra meningen är tillämplig.

När ett beslut ska upphävas

22 § Om det inte längre finns skäl för ett beslut om ingripande enligt denna lag ska den ingripande myndigheten omedelbart upphäva beslutet. Det gäller dock inte beslut om radering enligt 12 § som har genomförts.

Dokumentation

23 § Beslut och åtgärder enligt denna lag ska dokumenteras.

Bemyndigande

24 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. kompetenskrav enligt 11 och 13 §§,
2. underrättelser enligt 14 och 21 §§ och
3. medverkan och ersättning enligt 20 §.

---

1. Denna lag träder i kraft den 1 juli 2027.
2. Lagen upphör att gälla vid utgången av juni 2032.

1.2 Förslag till förordning (2027:000) om polisiära ingripanden i cybermiljö

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § I denna förordning finns kompletterande bestämmelser till lagen (2027:000) om polisiära ingripanden i cybermiljö. Begrepp och uttryck som används i förordningen har samma innebörd och tillämpningsområde som i lagen.

Kompetenskrav

2 § Polismyndigheten, Säkerhetspolisen och Tullverket ska utse en eller flera personer som får fatta beslut om ingripanden i cybermiljö enligt 11 och 13 §§ lagen (2027:000) om polisiära ingripanden i cybermiljö. Sådana personer ska ha goda kunskaper om digitala informationssystem och informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som är nödvändig och även i övrigt vara särskilt lämpade för uppdraget.

Polismyndigheten, Säkerhetspolisen och Tullverket ska även utse en eller flera personer som ska genomföra radering enligt 5 § lagen om polisiära ingripanden i cybermiljö. Sådana personer ska uppfylla kraven i första stycket.

3 § Myndigheten ska föra en förteckning över de personer som avses i 2 §.

Underrättelser

4 § Av en underrättelse till enskild enligt 14 § andra stycket andra meningen eller 21 § lagen (2027:000) om polisiära ingripanden i cybermiljö ska följande framgå

1. vilken myndighet som har gjort ingripandet,
2. vad ingripandet bestod i,

3. i vilket informationssystem eller användarkonto eller annan avgränsad del av ett informationssystem som ingripandet gjordes, och
4. när ingripande gjordes.

5 § Av en underrättelse enligt 14 § lagen (2027:000) om polisiära ingripanden i cybermiljö till Säkerhets- och integritetsskyddsnämnden vid Myndigheteten för säkerhet och integritetsskydd ska följande framgå
1. vilken myndighet som har gjort ingripandet,
2. vilket beslut om ingripande som har fattats,
3. vilken åtgärd som har vidtagits,
4. i vilket informationssystem eller användarkonto eller annan avgränsad del av ett informationssystem som åtgärden vidtogs,
5. när ingripandet gjordes, och
6. åklagarens ställningstagande.

6 § Om ett ingripande enligt lagen (2027:000) om polisiära ingripanden i cybermiljö riskerar att beröra en pågående förundersökning som leds av åklagare, ska samråd med åklagaren äga rum innan beslut om ingripande fattas.

Skyldighet att medverka

7 § Vid sådan medverkan som avses i 20 § lagen (2027:000) om polisiära ingripanden i cybermiljö ska den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation bistå den ingripande myndigheten enligt myndighetens begäran. Sådan medverkan kan omfatta att den anmälningspliktige
1. tillhandahåller tillgänglig teknisk information om det informationssystem som omfattas av beslutet,
2. tillhandahåller tillgängliga upplysningar om vilka förbindelser som används av det informationssystem som omfattas av beslutet,
3. använder tillgängliga tekniska metoder eller tillhandahåller möjlighet att använda sådana metoder, eller
4. tillhandahåller andra liknande tillgängliga åtgärder som kan användas för att genomföra ingripandet.

Bemyndigande om ersättning vid medverkan

8 § Post- och telestyrelsen får, efter att ha inhämtat synpunkter från Polismyndigheten, Säkerhetspolisen, Tullverket och Ekobrottsmyndigheten, meddela föreskrifter om ersättning enligt 20 § lagen (2027:000) om ingripanden i cybermiljö.

---

1. Denna förordning träder i kraft den 1 juli 2027.
2. Förordningen upphör att gälla vid utgången av juni 2032.

1.3 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

Lydelse enligt prop. 2025/26:147	*Föreslagen lydelse*
	1 §
Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd (nämnden) ska utöva tillsyn över	
1. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter,	
2. brottsbekämpande myndigheters användning av andra tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott än de som avses i 1, om inte den som åtgärden utförts hos eller annars riktats mot har närvarat vid åtgärden,	
3. brottsbekämpande myndigheters användning av en europeisk utlämnandeorder för trafikuppgifter eller innehållsdata enligt Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden,	
4. Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar, och	
5. därmed sammanhängande verksamhet.	
Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen och 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter.	
Nämnden ska också utöva tillsyn över Polismyndighetens och	Nämnden ska också utöva tillsyn över

Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.	*1.* Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott, *och* *2. brottsbekämpande myndigheters tillämpning av lagen (2027:000) om polisiära ingripanden i cybermiljö.*

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första–tredje styckena bedrivs i enlighet med lag eller annan författning.

Denna lag träder i kraft den 1 juli 2027.

1.4 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

Lydelse enligt 1.3	*Föreslagen lydelse*
	1 §
Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd (nämnden) ska utöva tillsyn över	
1. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter,	
2. brottsbekämpande myndigheters användning av andra tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott än de som avses i 1, om inte den som åtgärden utförts hos eller annars riktats mot har närvarat vid åtgärden,	
3. brottsbekämpande myndigheters användning av en europeisk utlämnandeorder för trafikuppgifter eller innehållsdata enligt Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden,	
4. Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar, och	
5. därmed sammanhängande verksamhet.	
Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen och 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter.	
Nämnden ska också utöva tillsyn över	Nämnden ska också utöva tillsyn över Polismyndighetens

1. Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott, *och*	och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.
2. brottsbekämpande myndigheters tillämpning av lagen (2027:000) om polisiära ingripanden i cybermiljö.	

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första–tredje styckena bedrivs i enlighet med lag eller annan författning.

Denna lag träder i kraft den 1 juli 2032.

1.5 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs att 9 kap. 4, 21 och 32 §§ lagen (2022:482) om elektronisk kommunikation ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 kap.	
4 §	
De begränsningar för behandling av trafikuppgifter som följer av 1–3 §§ gäller inte	
1. när en förvaltningsmyndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 1 § för att lösa tvister,	
2. för elektroniska meddelanden som omfattas av ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,	
3. för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *eller*	3. för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
	4. för elektroniska meddelanden som omfattas av ett beslut om ingripande enligt lagen (2027:000) om polisiära ingripanden i cybermiljö, eller
4. i den utsträckning uppgifter som avses i 1 § är nödvändiga för att förhindra eller avslöja	*5.* i den utsträckning uppgifter som avses i 1 § är nödvändiga för att förhindra eller avslöja

obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

21 §

Uppgifter som har lagrats enligt 19 § får behandlas endast för att lämnas ut enligt

1. 33 § första stycket 2 eller 5,	
2. 27 kap. 19 § rättegångsbalken, *eller*	2. 27 kap. 19 § rättegångsbalken,
3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *eller*
	4. lagen (2027:000) om polisiära ingripanden i cybermiljö.

32 §

Tystnadsplikt som följer av 31 § första stycket gäller även för en uppgift som hänför sig till

1. en åtgärd att med stöd av 27 kap. 9 § rättegångsbalken hålla kvar försändelser,

2. en angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller som gäller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,

3. en angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,

5. en begäran enligt 33 § första stycket 2 om att en uppgift om abonnemang ska lämnas,

6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift, *eller*

7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas.

6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,

7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas, *eller*

8. en begäran enligt 20 § lagen (2027:000) om polisiära ingripanden i cybermiljö.

Denna lag träder i kraft den 1 juli 2027.

1.6 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs att 9 kap. 4, 21 och 32 §§ lagen (2022:482) om elektronisk kommunikation ska ha följande lydelse.

Lydelse enligt 1.5	*Föreslagen lydelse*
9 kap.	
4 §	
De begränsningar för behandling av trafikuppgifter som följer av 1–3 §§ gäller inte	
1. när en förvaltningsmyndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 1 § för att lösa tvister,	
2. för elektroniska meddelanden som omfattas av ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,	
3. för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,	3. för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *eller*
4. för elektroniska meddelanden som omfattas av ett beslut om ingripande enligt lagen (2027:000) om polisiära ingripanden i cybermiljö, eller	
5. i den utsträckning uppgifter som avses i 1 § är nödvändiga för att förhindra eller avslöja	*4.* i den utsträckning uppgifter som avses i 1 § är nödvändiga för att förhindra eller avslöja

obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst

21 §

Uppgifter som har lagrats enligt 19 § får behandlas endast för att lämnas ut enligt

1. 33 § första stycket 2 eller 5,	
2. 27 kap. 19 § rättegångsbalken,	2. 27 kap. 19 § rättegångsbalken, *eller*
3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *eller*	3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.
4. lagen (2027:000) om polisiära ingripanden i cybermiljö.	

32 §

Tystnadsplikt som följer av 31 § första stycket gäller även för en uppgift som hänför sig till

1. en åtgärd att med stöd av 27 kap. 9 § rättegångsbalken hålla kvar försändelser,

2. en angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller som gäller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,

3. en angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,

5. en begäran enligt 33 § första stycket 2 om att en uppgift om abonnemang ska lämnas,	
6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,	6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift, *eller*
7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas, *eller*	7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas.
8. en begäran enligt 20 § lagen (2027:000) om polisiära ingripanden i cybermiljö.	

Denna lag träder i kraft den 1 juli 2032.

1.7 Förslag till lag om ändring i tullbefogenhetslagen (2024:710)

Härigenom föreskrivs i fråga om tullbefogenhetslagen (2024:710)

dels att rubriken till 7 kap. ska lyda Befogenheter för att upptäcka brott och göra vissa andra ingripanden,

dels att det ska införas en ny paragraf, 7 kap. 5 a §, och en ny rubrik före nya 7 kap. 5 a § med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	7 kap.
	Ingripanden i cybermiljö
	5 a §
	Bestämmelser om rätt för Tullverket att ingripa i cybermiljö finns i lagen (2027:000) om polisiära ingripanden i cybermiljö.

Denna lag träder i kraft den 1 juli 2027.

1.8 Förslag till lag om ändring i tullbefogenhetslagen (2024:710)

Härigenom föreskrivs i fråga om tullbefogenhetslagen (2024:710)

dels att rubriken till 7 kap. ska lyda Befogenheter för att upptäcka brott,

dels att 7 kap. 5 a § och rubriken före 7 kap. 5 a § ska upphöra att gälla.

Denna lag träder i kraft den 1 juli 2032.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Den 20 februari 2025 beslutade regeringen att tillsätta en särskild utredare med uppdrag att göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel i syfte att åstadkomma en mer effektiv och tydlig reglering och att förbättra möjligheterna att använda tvångsmedlen i brottsbekämpningens olika faser. Utredaren fick bl.a. i uppdrag att utvärdera tillämpningen av de utökade möjligheterna att använda hemliga och preventiva tvångsmedel och kartlägga den nytta som dessa inneburit för brottsbekämpningen i stort. I uppdraget ingick även att analysera behovet och nyttan av och att föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö, eller vidta andra jämförbara åtgärder i sådan miljö, i syfte att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot sådan brottslighet, och lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder (dir. 2025:12). Uppdraget skulle redovisas senaste den 29 maj 2026.

Genom tilläggsdirektiv den 26 mars 2026 beslutade regeringen att utredningstiden skulle förlängas och utredaren fick även vissa nya frågor att ta ställning till. Utredaren fick också i uppdrag att bl.a. analysera och ta ställning till om ett tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation och viss hemlig dataavläsning ska kunna knytas till en person i stället för till ett telefonnummer. Enligt tilläggsdirektivet ska uppdraget i stället redovisas senast den 1 februari 2027 (dir. 2026:20).

Den 28 maj 2026 beslutade regeringen genom ytterligare ett tilläggsdirektiv att uppdraget i den del som rör brott eller brottslig

verksamhet i cybermiljö ska förkortas. Uppdraget i den delen ska redovisas i ett delbetänkande, senast den 30 juni 2026 (dir. 2026:40).

Direktiven fogas som *bilaga 1*, *2* och *3* till betänkandet.

2.2 Utredningens arbete

Utredningen påbörjade sitt arbete i mars 2025. Det har bedrivits på sedvanligt sätt med regelbundna sammanträden med expertgruppen och löpande kontakter i enskilda frågor med experterna. Utredningen har hittills sammanträtt vid totalt 11 tillfällen.

Utredningen har för sitt arbete den 5 maj 2025 sammanträffat med företrädare för Tullverket (utredaren och två av sekreterarna), den 12 maj 2025 med företrädare för Åklagarmyndigheten (utredaren och sekreterarna), den 19 maj och 25 juni 2025 med företrädare för Polismyndigheten (utredaren och sekreterarna), den 23 maj och 16 juni 2025 med företrädare för Säkerhetspolisen (utredaren och sekreterarna) och den 27 januari 2026 med företrädare för Ekobrottsmyndigheten (utredaren och två av sekreterarna).

För den del av uppdraget som avser att föreslå åtgärder mot brott och brottslig verksamhet i cybermiljö har utredningen därutöver sammanträffat den 2 september 2025 med företrädare för Försvarets radioanstalt (utredaren och sekreterarna), den 22 oktober 2025 med företrädare för CERT vid Myndigheten för civilt försvar (utredaren och sekreterarna), den 13 april 2026 med företrädare för Nationellt cybersäkerhetscenter vid Försvarets Radioanstalt (utredaren och sekreterarna) och den 12 maj 2026 med företrädare för Myndigheten för säkerhet och integritetsskydd (utredaren och två av sekreterarna).

Utredningen har under andra delar av utredningsarbetet även sammanträffat med LSU-utredningen och med företrädare för Domarnämnden, för Sveriges advokatsamfund, för riksenheten för säkerhetsmål vid Åklagarmyndigheten och för statistikenheten vid Åklagarmyndigheten.

2.3 Betänkandets disposition

Författningsförslagen finns i kapitel 1 och i detta kapitel redovisas utredningens uppdrag och arbete. Kapitel 3–8 är deskriptiva kapitel, som ger en grundläggande förståelse för området och går igenom bl.a. skilda typer av brott i cybermiljö och olika lagstiftningsprojekt på området. I kapitel 9 tecknas en bild av brottsutvecklingen i cybermiljö. Kapitel 10 innehåller en redogörelse för hur cyberbrott bekämpas internationellt. De brottsbekämpande myndigheternas behov redovisas i kapitel 11. I kapitel 12 finns utredningens allmänna överväganden om ingripanden i cybermiljö och i kapitel 13 presenteras grundläggande frågor som rör den nya lagen om polisiära ingripanden i cybermiljö. Frågor om förutsättningarna för ingripanden, förbud mot ingripanden och vem som bör besluta om ingripanden behandlas i kapitel 14–16. Kapitel 17 tar bl.a. upp frågor om innehållet i beslut om ingripanden. Verkställighetsfrågor diskuteras i kapitel 18 och rättssäkerhetsgarantier i kapitel 19. Övriga frågor tas upp i kapitel 20. I kapitel 21 redovisas utredningens samlade bild av vilket integritetsintrång som förslagen kan leda till, hur de balanseras av förslagen om rättssäkerhetsåtgärder och hur förslagen förhåller sig till bl.a. Europakonventionen. Ikraftträdande och övergångsbestämmelser behandlas i kapitel 22. Därefter analyseras konsekvenserna av förslagen i kapitel 23. Författningskommentaren finns i kapitel 24.

3 Grundläggande rättighetsskydd

3.1 Bakgrund

En reglering som syftar till att störa och avbryta pågående brott och brottslig verksamhet i digital miljö riskerar att komma i konflikt med grundläggande fri- och rättigheter som gäller till skydd för privatlivet. Det grundläggande skyddet för privatlivet och den personliga integriteten som tillförsäkras enskilda regleras i bl.a. regeringsformen (RF) och den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Även i andra internationella instrument som är rättsligt bindande för Sverige finns det bestämmelser om skydd för privatlivet och den personliga integriteten.

3.2 Regeringsformen

RF, som är en av de svenska grundlagarna, slår bl.a. fast statsskickets grunder och de grundläggande fri- och rättigheterna. Av 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet. Enligt samma paragraf ska det allmänna värna den enskildes privatliv och familjeliv. Regleringen uttrycker en grundläggande målsättning för samhällets verksamhet.

I RF anges bl.a. att var och en är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp, kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande (2 kap. 6 § första stycket RF). Dessutom är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker

utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § andra stycket RF).

Skyddet enligt 2 kap. 6 § RF kan begränsas genom lag. En begränsning får enligt 2 kap. 20 och 21 §§ RF bara göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Dessutom får begränsningen aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen som en av folkstyrelsens grundvalar. Inte heller får en begränsning göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. Genom 2 kap. 21 § RF kommer proportionalitetsprincipen till uttryck.

Enligt 2 kap. 25 § RF är utlänningar här i landet jämställda med svenska medborgare när det gäller skyddet enligt 2 kap. 6 §.

3.3 Europakonventionen

Europakonventionen gäller, enligt lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, som svensk lag. Lag eller annan föreskrift får enligt 2 kap. 19 § RF inte meddelas i strid med Sveriges åtaganden enligt konventionen. Innebörden av konventionens artiklar uttolkas närmare av Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen) i Strasbourg.

I Europakonventionen regleras rätten till domstolsprövning och en rättssäker process i artikel 6. Vid prövningen av någons civila rättigheter eller skyldigheter eller av en anklagelse om brott ska var och en vara tillförsäkrad en rättvis och offentlig förhandling inom skälig tid och inför en oavhängig och opartisk domstol. I korthet är artikel 6, enligt Europadomstolens praxis, tillämplig under förutsättning att det föreligger en reell och seriös tvist mellan en enskild – fysisk eller juridisk – person och en annan person eller en myndighet, att tvisten gäller en rättighet eller skyldighet som har sin grund i den nationella rätten och att denna rättighet eller skyldighet kan karaktäriseras som civil (En moderniserad rättsprövning m.m., Ds 2005:9, s. 23).

Var och en har vidare rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Med korrespondens avses i Europa-

konventionen olika former för att överföra meddelanden mellan individer med hjälp av t.ex. telefon, telefax, radio och datorer. En offentlig myndighet får inte begränsa den rättigheten annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter (artikel 8).

Skyddet enligt artikel 8 är primärt en förpliktelse för staten att förhindra ingrepp i den skyddade rättigheten. Eftersom artikeln emellertid också ställer krav på att staten ska vidta positiva åtgärder för att skydda den enskildes privatsfär, såsom lagstiftning eller skydd mot övergrepp i särskilda situationer, kan staten bryta mot artikel 8 även om det inte har förekommit något ingripande från en myndighet eller en offentlig tjänsteman. Det kan vara fallet om staten inte har skapat ett tillräckligt rättsligt skydd. Staten kan på så sätt bli ansvarig för sin underlåtenhet, trots att det specifika intrånget i någon enskilds rättighet har utförts av någon annan enskild för vars handlande staten inte i och för sig är ansvarig (se t.ex. Europadomstolens dom den 12 november 2013 i Söderman mot Sverige, nr 5786/08, punkt 78).

Skyddet för privatliv är omfattande. Europadomstolen har flera gånger framhållit att det inte är möjligt att definiera begreppet genom en uttömmande beskrivning av olika aspekter som rör den enskildes privata förhållanden. Begreppet täcker olika aspekter av en enskild individs såväl fysiska som psykiska integritet (se exempelvis Europadomstolens dom den 3 april 2012 i Gillberg mot Sverige, nr 41723/06, punkt 66). Det följer också av artikeln att det ska finnas rättsmedel för att effektivt bekämpa brott, som utgör ett ingrepp i brottsoffrets rätt till privatliv.

När det gäller hemliga tvångsmedel kan särskilt noteras att det inte bara är privatlivet för personen som tvångsmedlet riktas mot som skyddas, utan även privatlivet för den som exempelvis ringer till en avlyssnad telefon. Avlyssningen i sig innebär ett ingrepp; det spelar ingen roll om inspelningarna aldrig ens har nått åklagaren utan har förstörts utan att ha använts (se Europadomstolens dom den 16 februari 2000 i Amann mot Schweiz, nr 27798/95, punkt 45, och Europadomstolens dom den 25 mars 1998 i Kopp mot Schweiz, nr 23224/94, punkterna 51–53).

I artikel 1 i tilläggsprotokoll nr 1 till Europakonventionen anges att var och en har rätt till respekt för sin egendom och att ingen får berövas sin egendom annat än i det allmännas intresse och under de förutsättningar som anges i lag och i folkrättens allmänna grundsatser.

3.4 Europeiska unionens rättighetsstadga

Även i Europeiska unionens stadga om de grundläggande rättigheterna (rättighetsstadgan) finns det bestämmelser om skydd för privat- och familjeliv och den personliga integriteten. Rättighetsstadgan, som tillkännagavs år 2000, blev rättsligt bindande år 2009 för EU:s medlemsstater.

Rättighetsstadgan är tillämplig på alla åtgärder som EU-institutionerna vidtar och medlemsstaterna ska följa den när de tillämpar och genomför unionsrätten. Det innebär att rättigheterna i stadgan endast måste iakttas vid tillämpningen av nationell lagstiftning som genomför EU-rätt och nationell lagstiftning som omfattas av unionens tillämpningsområde.

I rättighetsstadgan slås det bl.a. fast att var och en har rätt till fysisk och mental integritet (artikel 3), frihet och personlig säkerhet (artikel 6), respekt för sitt privat- och familjeliv, sin bostad och sina kommunikationer (artikel 7) samt skydd av de personuppgifter som rör honom eller henne (artikel 8).

Av artikel 52.3 följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som i konventionen, men att det inte hindrar unionsrätten från att tillförsäkra ett mer långtgående skydd. Stadgans rättigheter avseende barn och skydd för en enskilds personuppgifter har inte någon direkt motsvarighet i Europakonventionen.

3.5 FN:s konvention om medborgerliga och politiska rättigheter

FN:s generalförsamling antog år 1948 en allmän förklaring om de mänskliga rättigheterna. I artikel 12 i förklaringen slås fast att ingen får utsättas för godtyckliga ingripanden i fråga om bl.a. privatliv,

familj, hem eller korrespondens. Förklaringen är inte rättsligt bindande för staterna. Grundsatsen har emellertid även arbetats in i 1966 års FN-konvention om medborgerliga och politiska rättigheter (artikel 17). Artikeln trädde i kraft år 1976 och den är rättsligt bindande för konventionsstaterna. Sverige ratificerade konventionen den 26 november 1971 (SÖ 1971:42). FN:s kommitté för mänskliga rättigheter (MR-kommittén) granskar konventionsstaternas efterlevnad av konventionen. MR-kommittén avger allmänna kommentarer som bl.a. avser rekommendationer till konventionsstaterna och tolkning av konventionen.

3.6 Barnkonventionen

3.6.1 Allmänt

De grundläggande fri- och rättigheterna i RF och Europakonventionen gäller för alla, även för barn. Därutöver gäller barnkonventionen som svensk lag sedan den 1 januari 2020. Barnkonventionen ger alla barn upp till 18 år egna rättigheter (artikel 1). Rättigheterna är en del av de mänskliga rättigheter som under lång tid har fastställts i olika internationella överenskommelser. Dessa rättigheter är till sin karaktär odelbara och samverkande. Det innebär för barnkonventionens del att rättigheterna i konventionen, trots att de är av olika karaktär, bildar en helhet och förutsätter varandra. Rättigheterna gäller för varje barn, utan någon åtskillnad (Barnkonventionen blir svensk lag, SOU 2016:19, s. 88 f.).

FN:s kommitté för barnets rättigheter (Barnrättskommittén) övervakar efterlevnaden av barnkonventionen. Den består av oberoende experter. Konventionsstaterna avger vart femte år en rapport till kommittén om de åtgärder som de har vidtagit för att genomföra de rättigheter som erkänns i barnkonventionen och om de framsteg som gjorts i fråga om åtnjutandet av rättigheterna. Barnrättskommittén har gett ut allmänna kommentarer, bl.a. rekommendationer till konventionsstaterna och tolkning av barnkonventionen.

Barnkonventionen består av en inledning och tre avdelningar. I avdelning I behandlas de rättigheter barn har enligt konventionen och i avdelning II finns bestämmelser om efterlevnaden av konventionen, bl.a. Barnrättskommitténs uppdrag och staternas rapportering till kommittén. Slutbestämmelserna i avdelning III tar bl.a. upp

regler kring ratificering och ikraftträdande av konventionen. Avdelning I innehåller 41 artiklar och fyra av dem utgör konventionens s.k. grundprinciper.

3.6.2 Barnkonventionens grundprinciper

Barnkonventionens grundläggande principer är principen om icke-diskriminering (artikel 2), att barnets bästa alltid ska beaktas i första hand när åtgärder som gäller barn ska vidtas (artikel 3), barnets rätt till liv, överlevnad och utveckling (artikel 6) och rätten för barn att uttrycka sina åsikter och bli hörda (artikel 12). Grundprinciperna ska vara vägledande för hur övriga rättigheter i konventionen tolkas. Principerna har dessutom en självständig betydelse och ska vara utgångspunkt i beslut och åtgärder som kan röra enskilda barn eller grupper av barn. Barnrättskommittén har betonat vikten av att grundprinciperna återspeglas i den nationella lagstiftningen (Barnrättskommitténs allmänna kommentar CRC/GC/2003/5 p. 22).

3.6.3 Barns rätt till privat- och familjeliv

Artikel 16 behandlar barns rätt till skydd mot godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem och sin korrespondens samt mot olagliga angrepp på sin heder och sitt anseende. Den har följande lydelse:

> 1. Inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp på sin heder och sitt anseende.
> 2. Barnet har rätt till lagens skydd mot sådana ingripanden eller angrepp.

Rättigheterna i artikel 16 är inte absoluta utan får begränsas i lag. Vilka ingripanden som det kan röra sig om, utöver att de inte får vara godtyckliga eller olagliga, framgår inte av artikeln.

Barnrättskommittén har uttalat att stater, genom dialog med ungdomar, bör ta reda på var kränkningar av privatlivets helgd har skett, bl.a. när det gäller individens deltagande i den digitala miljön och hur företag och andra aktörer använder data (Barnrättskommitténs allmänna kommentar CRC/C/GC/20 p. 46).

Enligt MR-kommitténs allmänna kommentar till artikel 16 i konventionen om medborgerliga och politiska rättigheter ska uttrycket ”olagliga” tolkas så att varje ingripande måste ha stöd i lag. Begreppet ”godtyckliga” är enligt MR-kommittén avsett att garantera att de möjligheter till ingripande som föreskrivs i lag är förenliga med konventionens bestämmelser, syften och mål. Under alla omständigheter ska de vara rimliga i förhållande till de föreliggande omständigheterna. Lagstiftningen måste, enligt MR-kommittén, i detalj ange de exakta omständigheterna under vilka sådana ingripanden kan tillåtas, även om själva ingripandet stämmer överens med konventionen. MR-kommittén anser att ett beslut att utnyttja de lagliga möjligheterna till ingrepp i privatlivet endast får göras av en enligt lag behörig myndighet (MR-kommitténs allmänna kommentar, CCPR, nr 16 p. 4, 7–8 och 10).

Applicerat på barnkonventionen skulle det innebära t.ex. att ett ingrepp i ett barns privatliv endast får begränsa barnets tanke-, samvets-, religions- och yttrandefrihet om begränsningen är proportionerlig och syftar till att skydda den nationella säkerheten eller något av de andra intressen som anges i artiklarna 13 och 14. Samtidigt måste ingreppet vägas mot andra intressen enligt konventionen, t.ex. ska ett barn skyddas mot alla former av utnyttjande och övergrepp, även när barnet vårdas av sina föräldrar (artiklarna 19 och 32–36). Barnrättskommittén har bl.a. pekat på riskerna med informations- och kommunikationsteknologi i relation till våld mot barn. De nämner t.ex. nätmobbning eller att ett barn kan tvingas, luras eller övertalas att möta främlingar utanför internet och riskera att bli utsatta för grooming för sexuella syften och/eller lämna ut personlig information (Barnkonventionen och svensk rätt, SOU 2020:63, s. 634, Barnrättskommitténs allmänna kommentar CRC/C/GC/13 p. 31).

Vad som avses med privat- och familjeliv, hem och korrespondens framgår inte av artikel 16.1 och lämnas därmed i viss mån till respektive stat att avgöra.

När det gäller begreppet privatliv har MR-kommittén, i förhållande till motsvarande bestämmelse i konventionen om medborgerliga och politiska rättigheter, uttalat att skyddet för privatlivet är någonting som är relativt, beroende på det samhälle man lever i. Insamling och lagring av personuppgifter nämns av kommittén som exempel på sådant som behöver vara lagreglerat. Myndigheter bör enligt kommittén bara kunna begära information om en persons pri-

vatliv om myndigheten enligt lag är behörig och om informationen är väsentlig för samhällets intressen, så som de förstås enligt konventionen (MR-kommitténs allmänna kommentar, CCPR, nr 16 p. 7 och 10).

När det gäller familjeliv används begreppet familj (family) i den engelska originaltexten. Samma begrepp används i artikel 17 i konventionen om medborgerliga och politiska rättigheter. MR-kommittén betonar vikten av en bred definition av begreppet (MR-kommitténs allmänna kommentar, CCPR, nr 16 p. 5). Skyddet mot ingrepp i familjen eller familjelivet har koppling till flera andra artiklar i barnkonventionen, bl.a. artikel 5 om att staten ska respektera föräldrarnas rättigheter och skyldigheter att vägleda sitt barn, artikel 7 om ett barns rätt att bli vårdat av sina föräldrar, artikel 8 om rätt att behålla sina släktförhållanden, artikel 20 om alternativ omvårdnad och inte minst artikel 9 om att skilja ett barn från sina föräldrar. Ett skydd mot ingrepp i ett barns familjeliv bör också ses i relation till artikel 18 som föreskriver att det är föräldrarna som har huvudansvaret för ett barns uppfostran och utveckling.

Hem bör förstås som den plats där en person bor eller utför sina vardagliga sysslor enligt MR-kommittén. För ett barn skulle det vara dels där barnet bor, dels där barnet vistas för alternativ omvårdnad, t.ex. inackorderingshem, internatskolor, familjehem, särskilda ungdomshem, sjukhus m.m. (SOU 2020:63 s. 635 och MR-kommitténs allmänna kommentar, CCPR, nr 16 p. 5).

Att skyddas från ingrepp i sin korrespondens innebär, enligt MR-kommittén, att korrespondensen ska levereras till adressaten utan avlyssning och utan att öppnas eller läsas på annat sätt (MR-kommitténs allmänna kommentar, CCPR, nr 16 p. 8). Artikel 16 i barnkonventionen anger inte vilken typ av korrespondens som avses. Eftersom formerna för korrespondens ständigt utvecklas bör begreppet tolkas dynamiskt. Korrespondens kan således vara olika former av meddelanden, t.ex. i form av ljud, bild, skrift, punktskrift, teckenspråk eller elektroniska signaler. Utöver telefon, brev, e-post och vanligt tal bör exempelvis meddelanden på sociala medier omfattas. Den delen av artikel 16 bör också läsas tillsammans med artikel 13, som handlar om ett barns rätt till yttrandefrihet och att sprida information (SOU 2020:63 s. 636 med där gjord hänvisning).

4 Brott och brottslig verksamhet i cybermiljö

4.1 Bakgrund

4.1.1 Problemen med brott och brottslig verksamhet i cybermiljö

Allmänna utgångspunkter

Dagens samhälle präglas av att informationsteknik (it) genomsyrar i stort sett alla sektorer. Internet har skapat nya möjligheter att snabbt, enkelt och billigt ta del av, hämta in och distribuera stora mängder information. Köp av vissa konsumtionsvaror och tjänster görs till betydande del via internet. Dessutom kan olika former av utrustning fjärrstyras, om de är uppkopplade mot internet. Den ökade digitaliseringen ger stora fördelar för både myndigheter, företag och enskilda. Samtidigt skapas nya sårbarheter i samhället som kan utnyttjas både av kriminella och av främmande makt. En ökad användning av internet medför en förhöjd risk för att datorer och nätverk används som verktyg för att begå brott.

Mindre risk för upptäckt

I takt med att samhället har digitaliserats har även kriminaliteten flyttat in i den digitala miljön. Bakom det ligger bl.a. att brott kan begås utan att gärningsmannen är fysiskt på plats, vilket minskar risken för att bli upptäckt och kunna lagföras för brotten. Det är oftast betydligt svårare att knyta någon till brott som begås med hjälp av internet, eftersom det saknas fysiska spår av brottet som kan leda till att gärningsmannen avslöjas.

Till den minskade risken för upptäckt bidrar också förekomsten av anonymiseringsnätverk, vilket utredningen återkommer till (se avsnitt 4.1.2). På samma sätt som totalsträckskryptering[1] minskar de brottsbekämpande myndigheternas möjligheter att avlyssna elektronisk kommunikation, minskar förekomsten av anonymiseringsverktyg möjligheten för myndigheterna att spåra personer som begår brott i cybermiljö.

Den tekniska utvecklingen

I dagens uppkopplade samhälle har fler och fler elektroniska enheter (kylskåp, dammsugare, kameror m.m.) fått funktioner för att kunna kommunicera via internet. Många personer är över huvud taget inte medvetna om vilka tekniska funktioner som viss elektronik eller annan utrustning innehåller. Robotgräsklippare innehåller exempelvis kommunikationsfunktioner som möjliggör styrning, schemaläggning och spårning. Vidare innehåller moderna bilar, lastfordon och jordbruksmaskiner ofta funktioner som kan spåra fordonet. De kan även ha kamerafunktioner och andra tekniska möjligheter som kan vara intressanta att utnyttja både för brottsbekämpande myndigheter och för kriminella.

I takt med att allt fler enheter kopplas upp mot internet ökar risken för att tekniska sårbarheter som upptäcks kan utnyttjas för angrepp. Dessutom förblir många elektroniska enheter uppkopplade långt efter det att tillverkaren har slutat att erbjuda säkerhetsuppdateringar. Det gör att många sårbarheter aldrig åtgärdas och enheterna blir därmed lättare att utnyttja för angrepp.

Ju fler tekniska möjligheter det finns, desto mer sårbart blir samhället för angrepp via internet.

Bristen på tydlig jurisdiktion

En grundläggande fråga när det gäller brott och brottslighet i cybermiljö är var brottet eller brotten äger rum och vilka rättsliga möjligheter det finns att ingripa mot sådana brott. Cybermiljön är nämligen ett utmanande område för den internationella rättsordningen.

[1] Med totalsträckskryptering avses att information krypteras på avsändarens enhet och dekrypteras först på mottagarens enhet.

Det är en digital värld där anonymisering och avsaknaden av fysiska gränser riskerar att underminera de traditionella jurisdiktionsprinciperna som bygger på territoriell suveränitet. Det moderna cybersamhället kännetecknas av att gärningsman, brottsoffer, data och tekniska resurser inte sällan befinner sig i olika jurisdiktioner. Förhållandena kan dessutom förändras snabbt när data flyttas med hjälp av molntjänster, proxyservrar och anonymiseringsnoder. Det ställer krav på en annan syn på rättslig kontext, där cyberdomänen i högre grad kan likställas med t.ex. rymden i det avseendet att båda saknar traditionella gränser. Det finns ingen rättskälla som tydligt skiljer cybermiljön från den fysiska miljön i jurisdiktionshänseende. Cybermiljön omfattas av folkrättens ramar, även om tillämpningen kan vara tekniskt och politiskt utmanande.

Både ett generellt samhällshot och ett hot mot enskilda

De senaste åren har statliga aktörer som agerar för främmande makt i ökande utsträckning börjat använda servrar och routrar, som har angripits så att de kan fjärrstyras, för att skapa storskaliga anonymiseringsnätverk (se avsnitt 4.1.2). Syftet med det är att kunna agera dolt i digital miljö. Anonymiseringsnätverk, som ständigt ändrar form och storlek, används bl.a. av främmande makt i avancerade angrepp mot andra länder i syfte att hämta in skyddsvärd och för främmande makt begärlig information. De vill kunna förneka sin inblandning i sådana dolda operationer och få information skickad utan att bli upptäckta. Även vid angrepp mot samhällsviktig infrastruktur är det viktigt för angriparen att kunna förneka inblandning.

Fenomenet crime as a service är ett sätt att på digitala plattformar bl.a. ”annonsera” kriminella tjänster av olika slag och erbjuda hjälp med att genomföra vissa typer av brott. Det har i Sverige framför allt varit ett inslag i sådana sprängningar och skjutningar som har förknippats med konflikter mellan kriminella nätverk.

Företag, myndigheter och kommuner utsätts i ökande grad för olika typer av digitala angrepp mot sina nätverk, framför allt överbelastningsangrepp och utpressningsangrepp. Effekterna av sådana angrepp kan drabba inte bara den som primärt är måltavlan utan även offrets kunder och leverantörer och andra berörda.

Även enskilda utsätts för brott med hjälp av internet, exempelvis bedrägerier, eller genom att deras datorer och annan elektronisk utrustning utnyttjas för att begå brott. Vid bedrägerier kan t.ex. AI-genererade röster användas för att få måltavlan att tro att han eller hon talar med en för honom eller henne känd och pålitlig person.

Brottsligheten utnyttjar både mänskliga och tekniska svagheter

Det går trender i kriminalitet. De senaste åren har bl.a. utpressningsangrepp via internet blivit en populär inkomstkälla för organiserad brottslighet. Angrepp i cybermiljö har många olika former och utnyttjar såväl tekniska sårbarheter som mänskliga svagheter; allt från lösenordsangrepp och nätfiske till avancerade angrepp via tredjepartsleverantörer och mobila enheter. Enligt berörda myndigheter utvecklas hotbilden när det gäller cyberbrott ständigt. Genom att kombinera olika sorters angrepp kan angripare manipulera system, stjäla känslig information och orsaka stor skada för både myndigheter, organisationer och enskilda.

Cyberbrott kan få mycket stora konsekvenser

Det digitala samhället medför ofta beroenden mellan organisationer, vilket innebär att även mycket säkerhetsmedvetna verksamheter kan falla offer för cyberangrepp. Alla verksamheter är numera på ett eller annat sätt en del av det digitala systemet. Det innebär att incidenter som inträffar i miljöer som är utom den egna organisationens kontroll kan få stora negativa konsekvenser för den egna verksamheten. Det kan röra sig om allt från otillgängliga system, som negativt påverkar förmågan att tillhandahålla en viss tjänst, t.ex. Bank-id eller Freja, till utebliven leverans av exempelvis el eller vatten. Sådana händelser är svåra att helt skydda sig mot, eftersom alla verksamheter är beroende av leverantörer av olika tjänster och system.

It-incidenter som drabbar samhällsviktig verksamhet bedöms vara den typ av incidenter som kan leda till mest omfattande samhällspåverkan. Det gäller särskilt när många organisationer använder sig av samma it-leverantör.

Vissa aktörer sätter i system att kartlägga och planera intrång mot möjliga mål. Det varierar hur långsiktigt och fokuserat arbetet be-

drivs. Vissa angriper bara kända sårbarheter medan andra aktivt letar efter sårbarheter hos på förhand utvalda mål. Det finns också forum för kriminella där man köpslår om tillgång till utsatta objekts cybermiljöer. Tillgång till en cybermiljö som utsatts för angrepp kan utnyttjas på olika sätt beroende på drivkraften hos antagonisten.

Cyberangrepp drabbar som nämnts inte bara myndigheter, organisationer och företag utan även enskilda. De angrips ibland slumpvis, bl.a. genom nätfiske eller genom att deras personuppgifter och inloggningsuppgifter görs tillgängliga på internet och därigenom kan missbrukas. I andra fall inriktar sig kriminella på att kontakta personer som bedöms vara särskilt sårbara och förmår dem t.ex. att göra ekonomiska transaktioner eller vidta andra åtgärder som skadar dem.

Lagstiftningen har inte följt med utvecklingen

Lagstiftningen har successivt anpassats till att brott inte bara begås i den fysiska miljön utan även i den digitala. Till stora delar har den straffrättsliga och den straffprocessuella lagstiftningen moderniserats för att motverka brott i cybermiljö och att underlätta utredning av sådana brott. Däremot är den del av lagstiftningen som syftar till att brottsbekämpande myndigheter ska kunna upptäcka och ingripa mot brott alltjämt i allt väsentligt inriktad på den fysiska miljön.

4.1.2 Anonymiseringsnätverk

Vad ett anonymiseringsnätverk är

Anonymiseringsnätverk är en typ av nätverk som har byggts i syfte att dölja användarens it-trafik och identitet. Stora anonymiseringsnätverk är inget nytt fenomen och utnyttjas idag av många användare världen över. Det mest kända anonymisteringsnätverket TOR (The Onion Router) har funnits sedan millennieskiftet. TOR låter användare surfa och kommunicera anonymt. Nätverken används för både lagliga och olagliga aktiviteter. Medborgare och organisationer i länder som tillämpar censur av internet är en stor användargrupp, liksom kriminella.

Hur anonymiseringsnätverk kan användas

Anonymiseringsnätverk kan även byggas upp av statsunderstödda hotaktörer i syfte att genomföra cyberoperationer. Främmande makt använder anonymiseringsnätverk främst för att upprätta lager av informationsöverföringar som gör det nära nog omöjligt att spåra trafiken mellan avsändaren och målet och gör det möjligt för avsändaren att förneka sin inblandning. Ett anonymiseringsnätverk byggs upp av noder, dvs. knytpunkter som består av olika enheter (t.ex. en dator eller en server), som fungerar som mellanled för att vidarebefordra krypterad trafik. Den första noden i ett anonymiseringsnätverk är ofta en hyrd virtuell server. Ett vanligt tillvägagångssätt är att enheterna infekteras med skadlig kod som signalerar tillbaka till en kontrollserver. Från kontrollservern kan enheterna sedan administreras för att användas som noder i anonymiseringsnätverket. När det behövs kan kontrollservern skicka kommandon till de infekterade enheterna för att exempelvis få information eller uppdatera programvaran. Sådana tillvägagångssätt används troligen dels för att aktivera enheten som en nod för att slussa trafik i nätverket, dels för att infektera andra enheter och därmed utöka nätverket. Ofta används kända sårbarheter i vanligt förekommande program för att installera skadlig programvara på den infekterade enheten.

Anonymiseringsnätverken är designade för att skydda användarnas anonymitet, genom att trafiken dirigeras med metoder som gör det komplicerat att följa den. Nätverkens uppbyggnad gör det även enklare för dem som använder nätverken att smälta in bland normal trafik, vilket ökar deras möjlighet att dölja sina aktiviteter.

För kriminella innebär användning av anonymiseringsnätverk samma fördelar som nyss redovisats.

Vem som utsätts i anonymiseringsnätverk

Det finns två utsatta parter vid angrepp som utnyttjar anonymiseringsnätverk; dels den som äger den infekterade infrastrukturen, dels den som utgör det slutliga målet. Majoriteten av de infekterade enheterna finns hos privata användare och hos små och medelstora företag. Ägarna till enheterna är oftast omedvetna om att deras enheter utnyttjas på det beskrivna sättet.

Exempelvis utfördes under åren 2020 och 2021 omfattande cyberangrepp mot mål över hela Europa med hjälp av anonymiseringsnätverk. Angreppen var en del av en större kampanj som bedrevs av en kinesisk cybergruppering. Den använde ett nätverk av infekterade routrar som i första hand tillhörde privatpersoner i hela Europa. En del av den infrastruktur som gruppen byggde upp fanns i Sverige och i vissa fall skedde angrepp mot andra länder från routrar i Sverige.

4.2 Olika typer av cyberangrepp

4.2.1 Spridning av skadlig kod eller skadlig programvara

En av de allvarligaste formerna av cyberangrepp är att infektera datorer, nätverk och kommunikationsutrustning med skadliga uppgifter. Skadlig kod, eller skadlig programvara, infiltrerar och tar kontroll över ett datasystem eller en mobil enhet antingen för att stjäla värdefull information eller för att skada data och datasystem. Det finns många typer av skadlig kod och de kan komplettera varandra när de utför ett angrepp. Det gäller bl.a. följande.

- Ett botnet (som är en förkortning för robotnätverk) består av datorer som kommunicerar med varandra över internet. De utgörs ofta av kluster av infekterade enheter. En ”ledningscentral” använder dem för att skicka skräppost, utföra överbelastningsangrepp och begå andra brott.
- Ett rootkit är en samling program som ger tillgång på administratörsnivå till en dator eller ett datornätverk, vilket kan ge privilegierad tillgång till datorn och andra enheter i samma nätverk.
- En mask replikerar sig själv över ett datornätverk och utför skadliga åtgärder utan behov av styrning.
- En trojan utger sig för att vara, eller är inbäddad i, ett normalt program, men den är utformad för att skada, t.ex. att spionera, stjäla data, radera filer, expandera ett botnet och utföra överbelastningsangrepp.
- En bakdörr-trojan ger fjärrtillgång till ett datasystem eller en mobil enhet. Den ger angriparen en nästintill total kontroll genom att den kan utföra många olika åtgärder, bl.a. övervaka åtgär-

der, köra kommandon, skicka tillbaka filer och dokument, logga tangenttryckningar och ta skärmdumpar.

- En filinjektor infekterar filer genom att skriva över dem eller infoga en kod som inaktiverar dem.
- Ransomware hindrar användare från att komma åt information på sina enheter om de inte betalar en lösensumma för att få tillgång till enheterna igen.
- Scareware är ett falskt antivirusprogram som låtsas skanna och hitta en skadlig kod eller ett säkerhetshot på en användares enhet i syfte att förmå användarna att betala för att få det borttaget.
- Spionprogram installeras på datorer utan ägarens vetskap för att övervaka aktiviteten och överföra information till någon annan.

4.2.2 Överbelastningsangrepp

Ett överbelastningsangrepp, även känd som tillgänglighetsattack (Denial of Service, DoS), är ett försök att antingen överbelasta en tjänst eller ett nätverk för att försämra dess prestanda eller göra det otillgängligt för legitima användare. Sådana angrepp kan leda till avbrott i datasystem, vilket kräver både tid och resurser för återställning. Målet med angreppet är att göra tjänster otillgängliga, vilket kan påverka både användare och organisationer negativt.

Distribuerade överbelastningsangrepp (Distributed Denial of Service, DDoS) involverar flera källor som samtidigt genererar skadlig trafik. Det gör dem svårare att hantera eftersom de blandar sig med legitim trafik. Blockering av enskilda källor räcker då inte, utan det krävs mer sofistikerade motåtgärder.

4.2.3 Andra typer av cyberangrepp

Lösenordsangrepp

Angripare har gissat lösenord sedan datasystem kunde kopplas upp med modem på det sena 1980-talet. Lösenordens kvalitet är ofta låg, vilket gör att många kan forceras med hjälp av en vanlig bärbar dator. Användning av samma lösenord för ett flertal program eller applika-

tioner är ett särskilt vanligt problem, eftersom angripare ofta kan använda läckta lösenord från tidigare intrång.

Angrepp via e-post eller sms

E-post och sms används ofta vid nätfiske (phishing) eller, om angreppet är riktat mot specifika individer, i riktat nätfiske (spearphishing). Angripare kan skicka e-postmeddelanden eller sms som verkar äkta, för att lura mottagaren att klicka på länkar, öppna bifogade dokument eller tillåta hämtning av innehåll från internet. Genom sådana åtgärder kan angriparen bl.a. stjäla lösenord, kreditkortsuppgifter eller installera skadlig kod. Nätfiske och riktat nätfiske utnyttjar mänskliga svagheter som nyfikenhet, men också bristfällig implementering av tekniska skydd.

Nätfiske riktar sig mot en bred målgrupp och meddelandena saknar ofta detaljer. Det förekommer att angripare försöker träffa så många måltavlor som möjligt genom generiska meddelanden som påstår sig vara från betrodda aktörer. Det kan t.ex. vara fråga om falska meddelanden från myndigheter eller företag, som syftar till att förmå den som får meddelandet att kontakta den som står bakom utskicket.

Riktat nätfiske riktar sig mot specifika individer eller organisationer och inkluderar detaljer som namn eller information om mottagaren. Det kräver att angriparen kartlägger målet i förväg. Riktat nätfiske används ofta av statliga aktörer och kriminella, särskilt vid riktade trojanangrepp där några få måltavlor angrips.

Webbangrepp

Webbapplikationer består ofta av komplexa konstruktioner med flera lager av koder och abstraktioner, vilket skapar potentiella sårbarheter. Angripare kan t.ex. skicka en skadlig kod via ett webbformulär, som sedan körs i en databas. Det kan leda till att känslig information exponeras, att data ändras eller att obehöriga får tillgång till systemet.

Vattenhålsangrepp

Vattenhålsangrepp skiljer sig från nätfiske genom att angriparen inte kontaktar måltavlan direkt. I stället placeras en skadlig kod på en webbplats som är av intresse för målgruppen, exempelvis branschsidor eller lokala nyhetssidor. När användare besöker webbplatsen laddas koden ner till deras system, ofta utan deras vetskap. Det kan göras exempelvis genom att utnyttja sårbarheter i webbplattformen eller genom att manipulera tredjepartsinnehåll, som annonser.

Angrepp mot tredjepartsleverantörer

Tredjepartsleverantörer spelar en central roll i många organisationers leveranskedjor, vilket angripare utnyttjar. Angriparen infekterar en leverantörs system eller tjänster för att kunna skicka en skadlig kod i produkter eller tjänster som levereras till slutkunden. När kunden använder eller uppdaterar produkten sprids den skadliga koden direkt i företagets eller organisationens nätverk.

Angrepp mot mobila enheter

Mobiltelefoner och andra bärbara enheter är sårbara plattformar som kan utnyttjas i cyberangrepp för att samla in information. Om de angrips kan angripare få tillgång till en mängd känsliga uppgifter, bl.a. e-post, kreditkortsinformation, planerade resor, bilder, meddelanden, kontaktlistor och gps-positioner. Dessutom kan mobiltelefonens mikrofon användas för att avlyssna samtal och omgivande ljud.

Utpressningsangrepp

Ransomwareangrepp är en typ av utpressningsangrepp där information görs otillgänglig för verksamheten som drabbas. Det kan orsaka störningar i verksamheten, följdeffekter för medborgare eller kunder samt kostnader för hantering och begränsning av eventuell skada. Vanligtvis riktas krav mot den angripna verksamheten att betala en lösensumma, för att få tillbaka tillgången till den förlorade informationen. Ibland sker även s.k. exfiltrering, vilket innebär att informa-

tionen kopieras till en extern plats som hotaktören kontrollerar. I sådana fall kan hot om att offentliggöra information förekomma.

Några aktuella exempel är kommuner, vilkas it-system har blockerats, och applikationen Sportadmin, som används av många ideella föreningar och därför innehåller uppgifter om ett mycket stort antal personer. I det sistnämnda fallet publicerades uppgifterna från applikationen på Darknet, vilket medförde att skyddade personuppgifter röjdes i stor utsträckning.

Utpressningsangrepp kan genomföras på olika sätt. En alltmer vanlig form är Ransomware-as-a-Service (RaaS), vilket innebär att hela angreppet genomförs på beställning. Beställaren köper då en metod och väljer sedan själv måltavla och lösensumma. Beställaren sköter också kontakten med måltavlan och delar eventuella lösensummor med aktören bakom RaaS-tjänsten.

4.2.4 Fysiska angrepp

När informationssystem är svåra att nå via internet kan i stället personal utgöra ett säkerhetshot, genom att en individ kan utnyttja sin fysiska tillgång till sådana system. Det kan t.ex. röra sig om ett nätverk där någon för in en usb-sticka som innehåller skadlig kod, som kan spridas internt eller ge individen fjärrtillgång till nätverket.

Ett annat exempel är insiderhot, där en person, som antingen är rekryterad av angriparen eller är en missnöjd anställd, för in skadlig kod eller avslöjar känslig information inom en organisation. Insiderhot kan också skapas genom att utnyttja individers personliga förhållanden, exempelvis ekonomiska svårigheter eller sårbarhet för utpressning.

4.2.5 Kriminaliseringen av cyberangrepp är begränsad

Det är framför allt två straffbestämmelser som är särskilt utformade för att kriminalisera digitala angrepp. Det är dels bestämmelsen om dataintrång, dels bestämmelsen om datorbedrägeri. Även bestämmelsen om straffansvar vid överträdelse av lagen (1998:112) om ansvar för elektroniska anslagstavlor är relevant. Utredningen återkommer till den straffrättsliga regleringen i kapitel 5.

4.2.6 Cyberrelaterade brott av annat slag

Cyberbrott kan, som tidigare nämnts, innefatta en mängd olika typer av angrepp i cybermiljö som är direkt beroende av digitala informationssystem. Cyberbrott handlar dock inte bara om brott som riktas mot datorer och datatrafik, utan även om brott som begås med hjälp av informationssystem kopplade till internet men där brotten inte är direkt beroende av den digitala miljön, s.k. cyberrelaterade brott. Det kan t.ex. vara fråga om

- tvättning av traditionella och virtuella valutor och andra former av ekonomisk brottslighet, t.ex. bedrägerier,
- hot i nära relation där den tekniska utvecklingen har medfört nya möjligheter att övervaka och utöva kontroll över andra personer,
- olika former av sexuell exploatering av barn på internet, inklusive spridning av sexuellt övergreppsmaterial och direktsändning online av sexuella övergrepp mot barn,
- verksamhet online som involverar försäljning av falska pass, förfalskade och klonade kreditkort, narkotika och vapen och utannonsering av kriminella tjänster,
- rekrytering av barn och unga till kriminella nätverk online, och
- rekrytering till terrorism online.

Numera har enligt Polismyndigheten en mycket stor andel av alla brott åtminstone någon digital komponent. Det försvårar för myndigheten att fullgöra sitt uppdrag.

5 Den straffrättsliga regleringen

5.1 Dataintrång

5.1.1 Allmänt om straffbestämmelsen

Cyberbrott är inte något legalt begrepp. De olika formerna av angrepp i digital miljö som har beskrivits i kapitel 4 utgör i många fall dataintrång.

Enligt 4 kap. 9 c § första stycket brottsbalken döms den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Om brottet är grovt döms för grovt dataintrång. Straffskalan för det brottet är, från och med den 1 augusti 2026, fängelse i lägst ett år och högst åtta år (Dubbla straff för brott i kriminella nätverk och skärpta straffskalor, prop. 2025/26:218). Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art.

En förutsättning för straffansvar är alltså att handlingen utförs olovligen. Därmed utesluts från det straffbara området allt handlande med samtycke av den som har rätt att förfoga över uppgiften eller i överensstämmelse med gällande rätt, t.ex. regler om tvångsmedel (Angrepp mot informationssystem, prop. 2006/07:66, s. 17 och 23, se även NJA 2014 s. 221). I fråga om intrång genom blockering är exempelvis sedvanliga åtgärder som att testa ett systems säkerhet eller skydd eller att installera nya program alltså inte att anse som olovliga när de vidtas av behöriga personer i enlighet med behörigheten (prop. 2006/07:66 s. 50).

För straffansvar krävs inte att någon bereder sig tillgång till uppgiften i fråga i ett visst syfte eller att intrånget medför någon särskild effekt, exempelvis skada. Inte heller fordras det att någon säkerhetsåtgärd kringgås (prop. 2006/07:66 s. 18).

En förutsättning för straffansvar är däremot att gärningen begås uppsåtligen. Alla uppsåtsformer är tillämpliga (prop. 2006/07:66 s. 50).

Paragrafen om dataintrång är subsidiär i förhållande till straffbestämmelserna i 4 kap. 8 och 9 §§ brottsbalken om brytande av post- eller telehemlighet respektive intrång i förvar.

5.1.2 Avgränsningen till vissa uppgifter

Avsikten med begreppet ”uppgift som är avsedd för automatiserad behandling” är att förtydliga att alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form omfattas av bestämmelsen. Även dataprogram av olika slag omfattas. Det är utan betydelse var uppgifterna finns eller förvaras i systemet. Det innebär att alla uppgifter omfattas, oavsett på vilket datamedium de finns. Därmed innefattas också uppgifter som finns i en dators temporära minne. Även uppgifter som är under befordran omfattas. Det senare gäller oavsett på vilket sätt befordran sker. Beträffande uppgifter som befordras via radio gäller dock som regel att avlyssning av sådan kommunikation faller utanför det straffbara området. Det följer av principen om att etern är fri och av att olovlighetskravet därmed inte kan anses uppfyllt. Om intrånget däremot sker i radiobefordrade uppgifter som t.ex. är krypterade kan dock ansvar för dataintrång komma i fråga. Ansvar kan också komma i fråga för ändring eller utplånande av eller annan påverkan på radiobefordrade uppgifter som anges i paragrafen (prop. 2006/07:66 s. 49). Uppgifter som befordras i kommunikationsnät omfattas inte utan endast intrång i apparater för automatisk databehandling och i uppgifter som finns i sådana apparater för drift, användning, skydd och underhåll av dem (prop. 2006/07:66 s. 23).

5.1.3 Det straffbara handlandet

Bereda sig tillgång till, ändra och blockera

För straffansvar är det tillräckligt att någon ”bereder sig tillgång till” uppgifter som är avsedda för automatiserad behandling, dvs. att personen kan ta del av dem. Det krävs inte att han eller hon faktiskt tar del av uppgifterna. Bestämmelsen är tillämplig så snart någon olovligen har tagit sig in i en teknisk utrustning som används för uppgifter av sådant slag. Genom tillträdet till utrustningen har personen skaffat sig möjlighet att ta del av de uppgifter som finns i apparaten och alltså berett sig tillgång till dem (prop. 2006/07:66 s. 24).

En ”ändring” kan gälla den uppgift som databehandlas. En ändring kan också göras i det datorprogram som styr den aktuella databehandlingen. Ändringen kan vara bestående eller tillfällig. Att en uppgift ”utplånas” innebär att den helt eller delvis förstörs, t.ex. genom radering (prop. 2006/07:66 s. 18 f.). En åtgärd som innebär ändring eller utplåning kan, om den är mer omfattande och bestående, också utgöra skadegörelse enligt 12 kap. 1 § brottsbalken (prop. 2006/07:66 s. 12).

Med att någon ”blockerar” en uppgift som är avsedd för automatiserad behandling förstås åtgärder som innebär att en sådan uppgift görs oåtkomlig eller att den hindras från att flöda normalt. Det handlar alltså om hindrande eller spärrande åtgärder av olika slag. Exempel är inmatning eller spridning av olika typer av sabotageprogram (t.ex. datavirus eller trojaner). Det kan t.ex. handla om att programkod förs in i en dator och fyller minnesutrymmet med skräp, så att uppgifter inte kan nås eller lokaliseras. Om uppgifterna förändras eller förstörs, kan ansvar i stället komma i fråga för ändring eller utplånande av dem (prop. 2006/07:66 s. 50).

Föra in i register

Åtgärden att ”föra in i register” medför en begränsning av det straffbara området så att endast sådana införingar som görs i uppgifter strukturerade på visst sätt omfattas. Andra införingar kan dock vara straffbara genom att de träffas av de delar av bestämmelsen som straffbelägger ändring eller utplånande av och intrång i uppgifter (prop. 2006/07:66 s. 18).

Vidta annan åtgärd som allvarligt stör eller hindrar

Straffansvar kan också följa för den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling. Det straffbara förfarandet tar sikte på åtgärder som verkar så att de stör eller hindrar att uppgifterna kan användas på avsett sätt. Som exempel på sådana åtgärder kan nämnas överbelastningsangrepp. Det kan t.ex. handla om program som skapar och sänder så stora mängder e-post att mottagarens system kollapsar eller får kraftigt nedsatt funktion och därmed hindrar eller stör användningen av de uppgifter som finns i systemet. En sådan effekt kan också uppkomma till följd av manuella sändningar av e-post i stor skala. Som ytterligare exempel på åtgärder som kan verka på ett sådant sätt nämns i förarbetena upprepade kontakter eller försök till kontakter, införing av virusprogram eller annat sabotageprogram (prop. 2006/07:66 s. 50).

Med ”allvarligt stör” avses att det ska vara fråga om en betydande störning av inte endast tillfällig natur. Bedömningen av om en sådan störning har förelegat ska göras utifrån en helhetsbedömning. I det sammanhanget kan bl.a. sådana omständigheter som hur lång tid störningen har pågått och störningens art och omfattning vara av betydelse. Även andra omständigheter kan leda till en sådan bedömning. Med uttrycket ”hindrar” avses fall där användningen av en uppgift som är avsedd för automatiserad behandling helt avbryts eller förhindras. I det senare fallet torde dock som regel ansvar i stället inträda för blockering. Om en allvarlig störning eller ett hindrande orsakas av flera personer, krävs för straffansvar att den enskilde har uppsåt till den effekten (prop. 2006/07:66 s. 50).

Gärningsmannen ska ha åstadkommit den angivna effekten – allvarligt störande eller hindrande – genom en ”annan liknande åtgärd”. De åtgärder som avses ska alltså till sin art vara jämförbara med i första hand åtgärderna att ändra, utplåna, blockera eller i register föra in en uppgift. Som exempel nämns att överföra eller mata in en uppgift (prop. 2006/07:66 s. 51).

Utanför det straffbara området faller rena opinionsyttringar som innebär att meddelanden med visst åsiktsinnehåll sänds, t.ex. med e-post, till en mottagare för att denne ska ta del av innehållet och eventuellt låta sig påverkas av det. Det innebär t.ex. att en situation där flera personer på ett samlat och koncentrerat sätt uttrycker en

åsikt i e-post till en myndighet i sådan mängd att myndighetens datasystem havererar eller annars orsakas en betydande funktionsnedsättning faller utanför kriminaliseringen, om inte den enskilde i själva verket agerat med uppsåt att åstadkomma de angivna effekterna. Kriminaliseringen träffar inte heller fall där någon gör bruk av sin grundlagsfästa meddelarfrihet (prop. 2006/07:66 s. 51).

Osjälvständiga brottsformer

Försök och förberedelse till dataintrång som, om det fullbordats, inte skulle ha ansetts som ringa är straffbart enligt 4 kap. 10 § brottsbalken. Som exempel på förberedelse till dataintrång kan nämnas att ta befattning med en programvara som är konstruerad för att utföra överbelastningsangrepp. Även att sammanställa uppgifter inför t.ex. ett sådant angrepp om aktuell adress, tidpunkt och annat av betydelse för att genomföra brottet torde kunna föranleda ansvar för förberedelse till dataintrång, förutsatt att informationen är nedtecknad eller på annat sätt lagrad och att faran för brottets fullbordan inte har varit ringa (prop. 2006/07:66 s. 51).

5.2 Datorbedrägeri

5.2.1 Allmänt om bestämmelsen

Ett angrepp i digital miljö kan även utgöra s.k. datorbedrägeri enligt 9 kap. 1 § andra stycket brottsbalken.

Enligt 9 kap. 1 § första stycket brottsbalken döms för bedrägeri den som medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställe denne är, till fängelse i högst två år. Enligt andra stycket döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller uppgift eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan, för bedrägeri.

5.2.2 Olovlig påverkan

Med ”automatisk informationsbehandling” avses i första hand behandling i datorer. Lagstiftningen är dock teknikneutral, vilket innebär att även annan likartad utrustning faller under bestämmelsen (proposition med förslag till ändring i brottsbalken m.m. [vissa frågor om datorrelaterade brott och ocker], prop. 1985/86:65, s. 21). Den kan bl.a. avse bankomater och varuautomater, liksom påverkan på en automatisk verksamhet som tillhandahåller pengar, varor eller tjänster, exempelvis sedelutbetalnings-, varu- och bensinautomater (prop. 1985/86:65 s. 45).

Olovlig påverkan på den automatiska informationsbehandlingen kan göras på ett flertal olika sätt. Oriktiga eller ofullständiga uppgifter kan lämnas i den information som ska ligga till grund för behandlingen, oavsett om det gäller uppgifter i pappersdokument eller information via dataterminaler (prop. 1985/86:65 s. 18 och 44).

Med att någon olovligen ”ändrar i program”, dvs. i instruktionerna för den automatiska informationsbehandlingen, avses att byta ut hela programmet eller att flytta över programmet från ett bearbetningsställe till ett annat (prop. 1985/86:65 s. 44).

Med att olovligen ”ändra i en uppgift som är avsedd för automatisk informationsbehandling” avses i första hand olovliga förfaranden med datorer genom att lagrad data olovligen ändras eller helt eller delvis utplånas eller att nya data olovligen förs in i det material som ska bearbetas (prop. 1985/86:65 s. 45).

Bestämmelsen är tillämplig på i princip alla former av olovlig påverkan på resultatet av en automatisk process under förutsättning att förfarandet innebär en förmögenhetsöverföring. Skilda former av sådan olovlig påverkan ska således inte bedömas olika beroende av vilken teknisk konstruktion som apparaten eller anläggningen har. Exempelvis har oftast myntautomater en så enkel konstruktion att det kan framstå som främmande att hänföra den under begreppet automatisk informationsbehandling (prop. 1985/86:65 s. 21 och 45).

5.2.3 Förmögenhetsöverföring

För att brottet ska anses vara fullbordat ska gärningsmannen ha berett sig vinning och skada uppkommit för någon annan. Det sker ofta i och med att medel krediteras ett konto som disponeras av gär-

ningsmannen. Vinningen kan också uppkomma genom att gärningsmannen till följd av den automatiska informationsbehandlingen får tillgång till varor eller tjänster. Liksom när det gäller bedrägeri i allmänhet förutsätts att förmögenhetsöverföringen är en omedelbar följd av förfarandet. Förfarandet ska innebära, inte endast medföra, förmögenhetsöverföring (prop. 1985/86:65 s. 22).

5.2.4 Förhållandet till huvudregeln om bedrägeri

För ansvar enligt andra stycket i straffbestämmelsen om bedrägeri ställs inte, till skillnad från bedrägeri enligt första stycket, något krav på ett vilseledande, utan det är maskiner som utsätts för den påverkan som leder till förmögenhetsöverföring. För straffansvar är det tillräckligt att resultatet av informationsbehandlingen påverkas, så att det innebär vinning för gärningsmannen och skada för någon annan. Står det däremot klart att brottsrekvisiten även enligt första stycket är uppfyllda genom att en person först vilseleds och därefter fattar ett beslut som påverkar informationsbehandlingen, ska det dömas för bedrägeri enligt första stycket (prop. 1985/86:65 s. 24).

I 9 kap. 1 § andra stycket brottsbalken anges inte, till skillnad från första stycket, någon bestämd krets av skadelidande. Skadan torde dock i regel drabba den för vars räkning informationsbehandlingen eller processen i fråga har anordnats (prop. 1985/86:65 s. 44).

5.3 Lagen om ansvar för elektroniska anslagstavlor

5.3.1 Lagens tillämpningsområde

I lagen om ansvar för elektroniska anslagstavlor regleras vissa skyldigheter för den som tillhandahåller en elektronisk anslagstavla och straffansvar i de fall där skyldigheterna inte följs.

Med elektronisk anslagstavla avses i lagen en tjänst för elektronisk förmedling av meddelanden. Med meddelande avses enligt 1 § text, bild, ljud eller information i övrigt. I rättspraxis har lagen tillämpats på öppna kommentarsfunktioner på i övrigt statiska webbsidor (NJA 2007 s. 805 I) och på Facebook-grupper (Svea hovrätts dom den 4 december 2020 i mål B 8432–19). Vidare torde de sociala medieplattformarna ofta utgöra elektroniska anslagstavlor. I prakti-

ken kan ett och samma meddelande därför förmedlas på flera olika elektroniska anslagstavlor; dels på plattformen som sådan, dels i en grupp som tillhandahålls på plattformen. Med information i övrigt avses bl.a. datorprogram (Daniel Westman, Lagen (1998:112) om ansvar för elektroniska anslagstavlor, Karnov, 1 januari 2025, kommentaren till 1 §).

Enligt 2 § gäller lagen dock inte

1. tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden eller av andra anordningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse,
2. förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern,
3. tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,
4. meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (elektronisk post), eller
5. meddelanden som omfattas av TCO-förordningen.[1]

5.3.2 Straffansvar

Den som tillhandahåller en elektronisk anslagstavla ska enligt 4 § lagen om ansvar för elektroniska anslagstavlor, för att kunna fullgöra sin skyldighet enligt 5 §, ha sådan uppsikt över tjänsten som skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten. I 4 a § regleras vissa undantag från den skyldigheten för den som tillhandahåller en elektronisk anslagstavla som är en förmedlingstjänst enligt EU:s förordning om digitala tjänster. Tillhandahållaren bör regelbundet gå igenom innehållet i den elektroniska anslagstavlan. Vad som är ett rimligt tidsintervall får avgöras från fall till fall och främst med hänsyn till hur många som regelmässigt kopplar upp sig mot tjänsten. Det innebär i normalfallet att kravet bör sättas högre för tjänster som erbjuds yrkesmässigt än för tjänster som tillhandahålls av privatpersoner och som typiskt sett är mindre frekvent besökta. Ett riktmärke bör vara att en tjänst inte bör lämnas

[1] Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

utan tillsyn längre än en vecka (Ansvar för elektroniska anslagstavlor, prop. 1997/98:15, s. 15).

Enligt 5 § första stycket ska, om en användare sänder in ett meddelande till en elektronisk anslagstavla, den som tillhandahåller tjänsten ta bort meddelandet från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om innehållet i meddelandet avser något av följande brott: olaga hot, olaga integritetsintrång, uppvigling, hets mot folkgrupp barnpornografibrott, olaga våldsskildring eller offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet enligt terroristbrottslagen, eller intrång i upphovsrätt eller i en rättighet som skyddas genom föreskrift i 5 kap. lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.

Enligt 7 § första stycket döms den som uppsåtligen eller av grov oaktsamhet bryter mot 5 § första stycket till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år. I ringa fall ska det inte dömas till ansvar. Straffbestämmelsen är subsidiär till straffbestämmelser i brottsbalken och lagen om upphovsrätt till litterära och konstnärliga verk och terroristbrottslagen. För fullbordat brott krävs inte att någon spridning till andra användare faktiskt har ägt rum. Det räcker att meddelandet hålls tillgängligt för användare av tjänsten vid en tidpunkt när meddelandet borde ha avlägsnats (prop. 1997/98:15 s. 18 och 21).

6 Skyldighet att avlägsna visst innehåll

6.1 Bakgrund

Som redan nämnts finns det alltså viss lagstiftning som reglerar skyldighet att avlägsna visst innehåll online. När det gäller elektroniska anslagstavlor kan straffansvar komma i fråga för den som inte tar bort visst innehåll. Det finns emellertid också flera EU-rättsakter och kompletterande svensk lagstiftning som innehåller bestämmelser om sanktioner, som inte är straffrättsliga, för den som inte hörsammar ett föreläggande att ta bort visst digitalt innehåll. Vidare finns det förslag till en ny lagstiftning som syftar till att bekämpa rekrytering online till kriminella uppdrag, genom att förmå dem som tillhandahåller digitala plattformar att ta bort sådant innehåll.

6.2 Innehåll på elektroniska anslagstavlor

Enligt 5 § första stycket lagen om elektroniska anslagstavlor (se avsnitt 5.3 om lagen), ska, om en användare sänder in ett meddelande till en elektronisk anslagstavla, den som tillhandahåller tjänsten ta bort meddelandet från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om

1. meddelandets innehåll uppenbart är sådant som avses i bestämmelserna om
   a) olaga hot i 4 kap. 5 § brottsbalken,
   b) olaga integritetsintrång i 4 kap. 6 c § brottsbalken,
   c) uppvigling i 16 kap. 5 § brottsbalken,
   d) hets mot folkgrupp i 16 kap. 8 § brottsbalken,

e) barnpornografibrott i 16 kap. 10 a § brottsbalken,

f) olaga våldsskildring i 16 kap. 10 c § brottsbalken, eller

g) offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet i 7 § terroristbrottslagen, eller

2. det är uppenbart att användaren har gjort intrång i upphovsrätt eller i en rättighet som skyddas genom föreskrift i 5 kap. lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk genom att sända in meddelandet.

För att kunna fullgöra sin skyldighet har den som tillhandahåller tjänsten rätt att ta del av meddelanden som förekommer i tjänsten (5 § andra stycket). Skyldigheten enligt första stycket och rätten enligt andra stycket gäller också den som på tillhandahållarens uppdrag har uppsikt över tjänsten (5 § tredje stycket).

Tillhandahållaren ska ta bort meddelandet eller på annat sätt förhindra vidare spridning av meddelandet. Skyldigheten inträder när tillhandahållaren får kännedom om meddelandet.

Den som tillhandahåller en elektronisk anslagstavla ska enligt 4 § lagen om ansvar för elektroniska anslagstavlor, för att kunna fullgöra sin skyldighet att ta bort visst innehåll, ha sådan uppsikt över tjänsten som skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten. I 4 a § regleras vissa undantag från den skyldigheten för den som tillhandahåller en elektronisk anslagstavla som är en förmedlingstjänst enligt EU:s förordning om digitala tjänster. Tillhandahållaren bör regelbundet gå igenom innehållet i den elektroniska anslagstavlan. Vad som är ett rimligt tidsintervall får avgöras från fall till fall och främst med hänsyn till hur många som regelmässigt kopplar upp sig mot tjänsten. Det innebär i normalfallet att kravet bör sättas högre för tjänster som erbjuds yrkesmässigt än för tjänster som tillhandahålls av privatpersoner och som typiskt sett är mindre frekvent besökta. Ett riktmärke bör enligt förarbetena vara att en tjänst inte bör lämnas utan tillsyn längre än en vecka (prop. 1997/98:15 s. 15).

Skyldigheten att ta bort innehåll respektive rätten att ta del av innehållet gäller också för den som på tillhandahållarens uppdrag har uppsikt över tjänsten.

6.3 EU-lagstiftning om digitala tjänster

6.3.1 TCO-förordningen

Åtgärder för att motverka spridning av terrorisminnehåll

Som ett led i arbetet mot terrorism har EU vidtagit olika åtgärder för att motverka spridningen av terrorisminnehåll på internet, bl.a. genom att anta Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen). Förordningen syftar till att säkerställa att den digitala inre marknaden fungerar smidigt i ett öppet och demokratiskt samhälle genom att motverka att värdtjänster missbrukas för terrorismändamål och att bidra till den allmänna säkerheten i EU.

För att förordningen ska vara tillämplig krävs att det är fråga om spridning till allmänheten, dvs. tillgängliggörande av information på begäran av en innehållsleverantör (en användare av en värdtjänst som har tillhandahållit information som lagras eller sprids) för ett potentiellt obegränsat antal personer.

Terrorisminnehåll definieras som material som

a) anstiftar till att begå något av de brott som avses i artikel 3.1 a–i i terrorismdirektivet,[1] om sådant material, direkt eller indirekt, såsom genom förhärligande av terroristgärningar, förespråkar terroristbrott, och därigenom medför fara för att ett eller flera sådana brott kan begås,

b) värvar en person eller en grupp av personer för att begå något av de brott som anges i artikel 3.1 a–i i terrorismdirektivet eller bidrar till att något av dessa brott begås,

c) värvar en person eller en grupp av personer för att delta i en terroristgrupps verksamhet i den mening som avses i artikel 4 b i terrorismdirektivet,

d) tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen eller om andra specifika metoder,

[1] Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism (terrorismdirektivet).

e) tillhandahåller tekniker för att begå eller bidra till att begå något av de brott som avses i artikel 3.1 a–i i terrorismdirektivet, eller

f) utgör ett hot om att begå något av de brott som avses i artikel 3.1 a–i i terrorismdirektivet.

Material som sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller i syfte att förhindra eller bekämpa terrorism, inbegripet material som ger uttryck för polemiska eller kontroversiella åsikter inom ramen för den offentliga debatten, ska inte anses vara terrorisminnehåll (artikel 1.3).

Värdtjänstleverantörernas skyldigheter

Förordningen är tillämplig på värdtjänstleverantörer som erbjuder tjänster i EU. En värdtjänstleverantör levererar tjänster som består i att information som tillhandahållits av någon annan lagras på dennes begäran. En värdtjänstleverantör behöver inte ha sitt huvudsakliga verksamhetsställe i unionen för att förordningen ska vara tillämplig. Det räcker att leverantören erbjuder tjänster i unionen.

En behörig myndighet ska ha ett antal befogenheter, bl.a. att utfärda och granska avlägsnandeordrar, att övervaka genomförandet av specifika åtgärder och att påföra sanktioner.

En avlägsnandeorder innebär en skyldighet för en värdtjänstleverantör att avlägsna terrorisminnehåll eller göra det oåtkomligt i samtliga medlemsstater. Det ska göras så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern.

En avlägsnandeorder kan även riktas till en värdtjänstleverantör som varken har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i den medlemsstat där den utfärdande behöriga myndigheten finns. I sådana fall ska den utfärdande myndigheten samtidigt översända en kopia av avlägsnandeordern till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare. Den mottagande behöriga myndigheten har då möjlighet att granska ordern och under vissa förhållanden fastställa att den är oförenlig med TCO-förordningen eller de grundläggande rättigheter och friheter som garanteras i EU:s rättighetsstadga.

En värdtjänstleverantör som anses exponerad för terrorisminnehåll ska i sina användarvillkor inkludera och tillämpa bestämmelser om åtgärder mot missbruk av dess tjänster för spridning av terrorisminnehåll. Det är den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad som prövar om en leverantör ska anses exponerad för terrorisminnehåll. Ett beslut om att en värdtjänstleverantör är exponerad för terrorisminnehåll ska grundas på objektiva faktorer, t.ex. att värdtjänstleverantören under de föregående tolv månaderna har mottagit två eller fler avlägsnandeorder.

Värdtjänstleverantörerna ska bevara terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder eller andra specifika åtgärder, tillsammans med tillhörande data som är nödvändiga för att bl.a. förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott.

6.3.2 TCO-lagen

Lagen (2023:319) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll (TCO-lagen) innehåller kompletterande bestämmelser till förordningen.

Polismyndigheten, som har utsetts till svensk behörig myndighet, får enligt 4 § TCO-lagen förelägga en värdtjänstleverantör som åsidosätter någon av sina skyldigheter enligt vissa av artiklarna i TCO-förordningen att vidta sådana åtgärder som krävs för att värdtjänstleverantören ska uppfylla skyldigheten. Ett sådant föreläggande får förenas med vite.

TCO-lagen möjliggör även nödvändigt uppgiftsutbyte mellan Polismyndigheten och Säkerhetspolisen (12 § TCO-lagen).

6.3.3 Förordningen om en inre marknad för digitala tjänster

Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (EU:s förordning om digitala tjänster) innehåller bestämmelser om tjänsteleverantörers skyldigheter

att reagera om någon har använt tjänsten för att lagra visst olagligt eller annars olämpligt innehåll.

Det övergripande syftet med förordningen är att bidra till en korrekt fungerande inre marknad för förmedlingstjänster genom att fastställa harmoniserade regler för en säker, förutsebar och förtroendeskapande onlinemiljö som främjar innovation och i vilken de grundläggande rättigheterna i EU:s rättighetsstadga skyddas på ett effektivt sätt.

Förordningen tillämpas enligt artikel 2 på leverantörer av sådana förmedlingstjänster som erbjuds till tjänstemottagare i en eller flera medlemsstater, oavsett var de leverantörer som tillhandahåller förmedlingstjänsterna har sitt etableringsställe.

Förmedlingstjänster kan t.ex. vara infrastruktur för tredje parts innehåll, en vara eller en tjänst, t.ex. ett meddelande, en uppladdad video, ett blogginlägg eller en vara som bjuds ut till försäljning. Exempel på värdtjänster är molntjänster, webbhotell, avgiftsbelagda annonseringstjänster eller tjänster som möjliggör utbyte av information och innehåll online, inbegripen fillagring och fildelning (Kompletterande bestämmelser till EU:s förordning om digitala tjänster, prop. 2023/24:160, s. 19). Förmedlingstjänster kan tillhandahållas separat, som en del av en annan typ av förmedlingstjänst eller samtidigt med andra förmedlingstjänster.

De förmedlingstjänster som omfattas av förordningen är uteslutande tjänster för vidarebefordran, cachning, värdtjänster och mycket stora onlinesökmotorer.

En tjänst för enbart vidarebefordran är en tjänst som består av överföring i ett kommunikationsnät av information som tillhandahållits av en tjänstemottagare eller tillhandahållande av tillgång till ett kommunikationsnät.

Med cachningstjänst avses en tjänst som består av överföring i ett kommunikationsnät av information som tillhandahållits av en tjänstemottagare, som innefattar automatisk, mellanliggande och tillfällig lagring av informationen och som utförs enbart för att effektivisera vidare överföring av informationen till andra tjänstemottagare på deras begäran.

En värdtjänst är en tjänst som består av lagring av information som tillhandahålls av en tjänstemottagare och som görs på dennes begäran.

Tjänstemottagare definieras som en fysisk eller juridisk person som använder en förmedlingstjänst, i synnerhet för att söka information eller göra den tillgänglig.

Som huvudregel ansvarar leverantörer av förmedlingstjänster inte för information som tjänstemottagare tillhandahåller genom deras tjänster. Tjänsteleverantören har dock en skyldighet att, så snart den får kännedom om olaglig verksamhet eller olagligt innehåll, avlägsna det eller göra det oåtkomligt (artikel 6 i förordningen om en inre marknad för digitala tjänster).

6.3.4 Lagen med kompletterande bestämmelser till EU:s förordning om digitala tjänster

Lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster innehåller bestämmelser som kompletterar förordningen (1 §). I förordningen föreskrivs inte någon skyldighet för leverantörer av förmedlingstjänster att avlägsna olagligt innehåll. Förordningen ger inte heller rättsligt stöd för nationella behöriga myndigheter att förelägga en leverantör att ta bort sådant innehåll. Bestämmelser om vad som utgör olagligt innehåll och rätten att förelägga leverantörer av förmedlingstjänster att vidta åtgärder mot sådant innehåll eller att tillhandahålla viss specifik information regleras i annan unionsrätt eller i medlemsstaternas nationella rätt. Förordningens bestämmelser om förelägganden att agera mot olagligt innehåll och att tillhandahålla information reglerar endast medlemsstaternas skyldighet att säkerställa att föreläggandena utformas i enlighet med vissa formella krav och att utfärdade förelägganden hanteras och följs upp på visst sätt (prop. 2023/24:160 s. 20).

Om leverantörer av värdtjänster får kännedom om information som ger upphov till misstanke om att ett brott som inbegriper ett hot mot en eller flera människors liv eller säkerhet har skett, håller på att ske eller sannolikt kommer att ske, ska de anmäla det till brottsbekämpande eller rättsliga myndigheter. Av 2 kap. 3 § lagen med kompletterande bestämmelser till EU:s förordning om digitala tjänster framgår att en sådan anmälan ska göras till Polismyndigheten. Värdtjänstleverantören bör då tillhandahålla all relevant information som den har tillgång till (prop. 2023/24:160 s. 114).

6.3.5 Direktivet om bekämpning av våld mot kvinnor och våld i nära relationer

I Europaparlamentets och rådets direktiv (EU) 2024/1385 av den 14 maj 2024 om bekämpning av våld mot kvinnor och våld i nära relationer finns bestämmelser om åtgärder för att ta bort visst online-material. Syftet med direktivet är att fastställa en heltäckande ram för att effektivt bekämpa våld mot kvinnor och våld i nära relationer inom EU. Direktivet ställer bl.a. krav på att alla medlemsstater kriminaliserar kvinnlig könsstympning, tvångsäktenskap och brott på internet, bl.a. nättrakasserier och delning av intima eller manipulerade bilder utan samtycke och offentlig uppmaning till våld eller hat på internet (artiklarna 3–8). Brotten ska beläggas med effektiva, proportionerliga och avskräckande straffrättsliga påföljder (artikel 10). Direktivet ålägger också medlemsstaterna att vidta lämpliga åtgärder för att förebygga våld mot kvinnor och våld i nära relationer och fastställer standarder för skydd och stöd till brottsoffer.

Artikel 23 innehåller bestämmelser om åtgärder för att avlägsna visst onlinematerial. Enligt artikeln ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att visst material som är allmänt tillgängligt online skyndsamt avlägsnas eller görs oåtkomligt. Det handlar om material som

1. visar handlingar med uttrycklig sexuell innebörd eller en persons intima kroppsdelar eller manipulerat sådant material som gjorts tillgängligt för allmänheten utan personens samtycke, och
2. utgör vissa former av nättrakasserier eller uppmaning till våld eller hat mot en grupp personer eller en medlem av en grupp, utpekad med åberopande av kön.

De åtgärder som medlemsstaterna enligt direktivet ska vidta ska innefatta en möjlighet för behöriga myndigheter att utfärda bindande rättsliga förelägganden mot värdtjänstleverantörer att avlägsna sådant material eller göra det oåtkomligt.

Materialet ska göras oåtkomligt utan angivande av territoriellt område. Om avlägsnande inte är möjligt får de behöriga myndigheterna även rikta förelägganden mot vissa andra leverantörer av förmedlingstjänster att vidta åtgärder i fråga om det berörda materialet.

Med tanke på att det material som kan behöva avlägsnas eller göras oåtkomligt kan ha betydelse för att utreda eller lagföra brott

kan emellertid krav på att de behöriga myndigheterna t.ex. ska bevara materialet under en begränsad period som inte är längre än nödvändigt behöva införas i nationell lagstiftning (skäl 55).

En utredning om genomförande av direktivet i svensk rätt pågår (Ju 2025:07).

6.4 Förslag till lag om avlägsnande av rekryteringsinnehåll online

I propositionen Nya möjligheter att bekämpa onlinerekrytering (prop. 2025/26:276) föreslås en ny lag om avlägsnande av rekryteringsinnehåll online. Lagen, som föreslås träda i kraft den 15 juli 2026, syftar dels till att motverka onlinerekrytering till brottslighet, av inte minst barn och ungdomar, dels till att bekämpa fenomenet crime as a service.

Lagen möjliggör för en behörig myndighet att besluta förelägganden om att innehåll online som syftar till att rekrytera personer för att begå brott (rekryteringsinnehåll) ska avlägsnas eller göras oåtkomligt (1 och 5 §§). Med rekryteringsinnehåll avses innehåll som skäligen kan antas utgöra ett led i en straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer eller involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken (2 §).

Ett föreläggande om avlägsnande ska riktas till den som tillhandahåller den plattform (värdtjänst), som omfattas av förordningen om digitala tjänster (5 §). Det innebär att föreläggandet ska riktas till den som tillhandahåller den tjänst där informationen finns, inte till den som har skapat innehållet eller lagt ut det på internet. En sådan avgränsning träffar alltså den krets av aktörer, tex. plattformar för social media eller för delning av innehåll, som normalt bör ha möjlighet att ta bort innehållet (prop. 2025/26:276 s. 38). Lagen gäller endast rekryteringsinnehåll som riktar sig till svenska medborgare eller personer som har hemvist i Sverige, görs tillgängligt av någon som befinner sig i Sverige eller avser brott som ska begås i Sverige eller mot en svensk medborgare eller någon som har hemvist i Sverige (3 §). Innehållet ska avlägsnas eller göras oåtkomligt så snart som möjligt och senast inom en timme efter det att föreläggandet har tagits emot (7 §). Utgångspunkten är att rekryteringsinnehåll

ska avlägsnas eller göras oåtkomligt utan begränsning till visst territoriellt område. Eftersom lagen avgränsas till leverantörer av värdtjänster som omfattas av förordningen om digitala tjänster kommer det endast att bli fråga om att göra material oåtkomligt i en eller flera av EU:s medlemsstater (prop. 2025/26:276 s. 42 f.). Lagen gäller inte innehåll som omfattas av TCO-förordningen (4 §). En värdtjänstleverantör ska bevara rekryteringsinnehållet, med tillhörande data, i sex månader från det att innehållet avlägsnats eller gjorts oåtkomligt (8 §). En sådan skyldighet motiveras av att materialet kan behövas för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott (prop. 2025/26:276 s. 44.). Sanktionsavgift ska kunna tas ut av en värdtjänst som överträder sina skyldigheter enligt lagen (9–14 §§).

7 Budapestkonventionen

7.1 Konventionen om it-relaterad brottslighet

7.1.1 Allmänt om konventionen

Europarådets konvention om it-relaterad brottslighet (ETS 185, kallad Budapestkonventionen) utarbetades för att tillgodose behovet av en samordnad, effektiv kamp över gränserna mot it-relaterad brottslighet (Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet, prop. 2020/21:72, s. 19). Konventionen öppnades för undertecknande år 2001 och trädde i kraft den 1 juli 2004. I dag har 82 stater ratificerat konventionen och ytterligare 2 stater har undertecknat den. Konventionen trädde i kraft den 1 augusti 2021 gentemot Sverige.

Konventionen har tre huvudsyften. Det första syftet är att åstadkomma en tillnärmning av ländernas straffrätt beträffande följande gärningar: olagligt intrång, olaglig avlyssning, datastörning, systemstörning, missbruk av apparatur, datorrelaterad förfalskning, datorrelaterat bedrägeri, barnpornografibrott och brott som hänför sig till intrång i upphovsrätt och närstående rättigheter. Det andra syftet är att säkerställa att det finns nationella processrättsliga bestämmelser för att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta tillvara bevisning i elektronisk form. Det tredje syftet är att främja ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott.

Konventionen är indelad i fyra kapitel. De innehåller definitioner (kapitel I), bestämmelser om straff- och processrättsliga åtgärder som ska vidtas på nationell nivå (kapitel II), bestämmelser om internationellt samarbete (kapitel III) och slutbestämmelser (kapitel IV).

I kapitel II ställs krav på kriminalisering av vissa gärningar som begås med hjälp av ett datasystem. Vidare ställs krav på att medlemsstaterna ska kunna vidta olika processrättsliga åtgärder vid utredning av de brott som omfattas av konventionen. Det finns även regler om domsrätt.

Bestämmelserna om internationellt samarbete utgör en betydande del av konventionen. Kapitlet är uppdelat i ett allmänt avsnitt, där de grundläggande principerna för samarbetet läggs fast, och ett avsnitt med särskilda bestämmelser om rättslig hjälp.

7.1.2 Tilläggsprotokollen

Ett första tilläggsprotokoll till Budapestkonventionen (ETS 189) öppnades för undertecknande i januari 2003 och trädde i kraft den 1 mars 2006. Hittills har 38 stater ratificerat tilläggsprotokollet och ytterligare 9 stater har undertecknat det.

Det första tilläggsprotokollet är uppbyggt på samma sätt som konventionen med gemensamma bestämmelser (kapitel I), bestämmelser om straffrättsliga åtgärder (kapitel II), bestämmelser om förhållandet mellan konventionen och tilläggsprotokollet (kapitel III) och slutbestämmelser (kapitel IV).

I kapitel II ställs krav på kriminalisering av vissa gärningar av rasistisk och främlingsfientlig natur som begås med hjälp av datasystem. Tillämpningsområdet för konventionens processrättsliga bestämmelser och bestämmelserna om internationellt samarbete utvidgas till att omfatta de brott som omfattas av tilläggsprotokollet.

Det andra tilläggsprotokollet (CETS 224) öppnades för undertecknade den 12 maj 2022 och träder i kraft efter att fem konventionsstater har ratificerat protokollet. Hittills har 4 stater ratificerat tilläggsprotokollet och ytterligare 48 stater har undertecknat det. Det syftar till att ge brottsbekämpande myndigheter nya och effektivare verktyg för gränsöverskridande tillgång till elektroniska bevis.

Det andra tilläggsprotokollet innehåller gemensamma bestämmelser (kapitel I), bestämmelser om åtgärder för utökat samarbete (kapitel II), bestämmelser om villkor och garantier, inklusive dataskydd, (kapitel III) och slutbestämmelser (kapitel IV).

I kapitel II regleras bl.a. allmänna principer och att behöriga myndigheter i en konventionsstat ska kunna vända sig till privata aktörer

i en annan konventionsstat för att få ut domännamns- och abonnemangsuppgifter. Behöriga myndigheter i en stat ges möjlighet att vända sig till behöriga myndigheter i den andra staten för verkställighet av en order om utlämnade av abonnemangs- och trafikuppgifter med extra skyndsamhet. Vidare regleras påskyndat utlämnande av lagrade datorbehandlingsbara uppgifter i en nödsituation via det 24/7-nätverk som inrättats genom konventionen och under vilka omständigheter en stat kan ansöka om rättslig hjälp enligt ett skyndsamt förfarande i en nödsituation. Även förfarandet vid internationellt samarbete i brist på tillämpliga internationella avtal regleras.

Sverige har undertecknat båda tilläggsprotokollen och ratificerat det första.

7.2 Implementeringen av Budapestkonventionen och tilläggsprotokollen

7.2.1 Sveriges tillträde till Budapestkonventionen och det första tilläggsprotokollet

Inför Sveriges tillträde till Budapestkonventionen och det första tilläggsprotokollet konstaterade regeringen att svensk rätt redan uppfyllde konventionens och tilläggsprotokollets krav på straffrättsliga bestämmelser, men att lagändringar var nödvändiga för att uppfylla vissa av kraven i fråga om den processrättsliga regleringen och internationellt samarbete (prop. 2020/21:72 s. 20 och 50 f.). Det gällde kraven i artikel 16 om skyndsamt säkrande av lagrade uppgifter, i artikel 17 om skyldighet att lämna ut information om tillhandahållare som deltagit i överföringen av uppgifterna och i artikel 29 om ömsesidig rättslig hjälp.

7.2.2 Genomförandet av artikel 16

Säkrande av vissa uppgifter genom föreläggande

Brottsutredande myndigheter ska enligt konventionen ha möjlighet att skyndsamt säkra särskilt angivna datorbehandlingsbara uppgifter som redan är lagrade (artikel 16.1). Artikeln syftar till att ge brottsutredande myndigheter möjlighet att under en begränsad tidsperiod

säkra lagrade datorbehandlingsbara uppgifter i avvaktan på ett eventuellt beslut om andra tvångsåtgärder, en form av s.k. frysning. Ett föreläggande ska kunna riktas mot den som innehar uppgifterna.

Artikel 16.1 har genomförts genom 27 kap. 16 § RB. Enligt första stycket i paragrafen får den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott föreläggas att bevara uppgiften. Att uppgiften skäligen kan antas ha betydelse för utredningen är ett relativt lågt krav på uppgiftens betydelse ur bevissynpunkt. Det behöver inte finnas någon som är misstänkt för brottet. Föreläggandet behöver inte heller kopplas till en viss typ av brott eller till brott av en viss svårhetsgrad.

De uppgifter som avses kan vara av vilket slag som helst, t.ex. en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat. Att uppgiften ska vara lagrad betyder att den ska finnas bevarad elektroniskt. Både sådana uppgifter som har lagrats på grund av regler om datalagring och sådana som har lagrats av annan anledning omfattas. Regleringen innebär ingen skyldighet att lagra elektronisk information. Uppgiften måste vara lagrad när föreläggandet meddelas. Det är alltså inte tillåtet att förelägga någon att i framtiden lagra eller spara uppgifter. I föreläggandet ska det anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande får därmed inte vara generellt och endast ange att alla uppgifter som mottagits under en viss tid ska bevaras (prop. 2020/21:72 s. 23 och 68).

Proportionalitetsprincipen gäller även för den nu aktuella åtgärden. Den innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet alltid ska stå i rimlig proportion till vad som står att vinna med den. Ett föreläggande om bevarande får inte meddelas om det inte finns ett tillräckligt starkt behov av åtgärden med beaktande av motstående intressen och föreläggandet ska upphävas när åtgärden inte längre kan anses vara proportionerlig (prop. 2020/21:72 s. 26 och 68).

Vem föreläggandet får riktas mot

Ett föreläggande får riktas mot fysiska eller juridiska personer som innehar uppgifterna. Uppgifterna ska antingen finnas lagrade hos personen eller på annat sätt vara åtkomliga för personen. I det senare fallet kan uppgifterna lagras på en server någon annanstans än där personen befinner sig. Lagrade uppgifter kan också innehas av flera olika personer samtidigt, t.ex. om en person har sin e-post lagrad på en server hos en annan person. Ett föreläggande kan då riktas mot såväl den hos vilken uppgifterna finns lagrade som den som på distans har tillgång till uppgifterna (prop. 2020/21:72 s. 24 f. och 68).

Innehållet i föreläggandet

Den som innehar en viss lagrad elektronisk uppgift får åläggas att se till att uppgiften bevaras på ett sådant sätt att den inte kan förstöras, förändras eller på annat sätt göras oåtkomlig. Föreläggandet bör som huvudregel ges skriftligen. Det kan även finnas behov av att meddela ett föreläggande muntligt, exempelvis om ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande. Då behöver föreläggandet dokumenteras skriftligt och tillställas den som har förelagts åtgärden så snart det är möjligt. Eftersom föreläggandet avser en viss uppgift ska det anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Det finns flera möjliga sätt att efterkomma ett föreläggande, t.ex. genom kopiering av uppgiften eller genom att vidta åtgärder för att uppgiften ska lämnas orubbad på sin ursprungliga plats. Vid behov får den som beslutar om föreläggandet ge anvisningar om hur uppgiften ska bevaras i det enskilda fallet (prop. 2020/21:72 s. 27 och 68).

I föreläggandet ska det anges hur länge uppgiften ska bevaras. Tiden får inte bestämmas till längre än nödvändigt och får inte överstiga 90 dagar från dagen för beslutet. Om det finns särskilda skäl får tiden förlängas med ytterligare högst 90 dagar.

Enligt 27 kap. 16 § fjärde stycket RB får ett föreläggande inte riktas mot den som skäligen kan misstänkas för brottet eller mot någon sådan närstående person till honom eller henne som avses i 36 kap. 3 § RB. Föreläggandet ska upphävas om den som har förelagts att

bevara en viss uppgift blir skäligen misstänkt för det brott som utreds (prop. 2020/21:72 s. 69).

I 27 kap. 16 a § andra stycket RB föreskrivs att det i föreläggandet ska anges att den som ska bevara en viss uppgift inte får uppenbara att åtgärden har vidtagits. Det innebär inte att tystnadsplikten har företräde framför den grundlagsskyddade rätten att meddela och offentliggöra uppgifter. Yppandeförbudet är en del av föreläggandet och gäller som huvudregel till dess att föreläggandet inte längre gäller, rätten har upphävt föreläggandet eller åklagaren eller undersökningsledaren har meddelat något annat (prop. 2020/21:72 s. 29).

Beslutsfattare och prövning av föreläggandet

Säkrandet av uppgifter ska ske skyndsamt. Ett föreläggande enligt 27 kap. 16 § RB får beslutas av undersökningsledaren eller en åklagare (27 kap. 16 a § första stycket RB). Skälet till det är enligt förarbetena behovet av att snabbt kunna säkra en viss lagrad uppgift för att kunna bedriva effektiva brottsutredningar. Regleringen är även tillämplig i de fall där Tullverket eller Kustbevakningen har inlett en förundersökning.

Enligt 27 kap. 16 a § tredje stycket RB får den som har förelagts att bevara en viss uppgift begära rättens prövning av föreläggandet. Vid rättens prövning ska 27 kap. 6 § första stycket RB tillämpas. Den paragrafen reglerar rättens prövning av beslag. Både förläggandet i sig och tiden för bevarande kan prövas av rätten (prop. 2020/21:72 s. 29 f.). Enligt den arbetsfördelning som finns mellan åklagare och undersökningsledare vid andra myndigheter, ska ledningen av förundersökningen övertas av åklagare om föreläggandet har utfärdats av någon annan än åklagare. Frågan om uppgiften ska fortsätta att bevaras ska avgöras med utgångspunkt i förhållandena vid rättens prövning (prop. 2020/21:72 s. 70).

Sanktioner

Det konstaterades i förarbetena att konventionen inte kräver att det införs några sanktioner mot den som inte följer ett föreläggande om bevarande. Straffbestämmelsen om överträdelse av myndighets bud (17 kap. 13 § brottsbalken) bör dock kunna tillämpas i fall där någon

aktivt raderar en uppgift i strid med ett föreläggande om att bevara den. Även den som medverkar till ett sådant brott kan dömas till ansvar enligt 23 kap. 4 § brottsbalken. Brott mot yppandeförbudet kan föranleda straffansvar enligt 9 kap. 6 § RB (prop. 2020/21:72 s. 30).

7.2.3 Genomförandet av artikel 17

Uppgifter ska lagras

Ett säkrande av lagrade uppgifter ska enligt artikel 17 i konventionen vara möjligt oavsett om en eller flera tjänsteleverantörer har deltagit i överföringen av uppgifterna. Det förutsätter att det går att identifiera vilka tjänsteleverantörer som har deltagit i överföringen. Enligt förarbetena behöver elektroniska uppgifter kunna säkras hos tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster för att uppfylla kraven i artikel 17. Därför ändrades bestämmelserna i dåvarande 6 kap. 8 § lagen (2022:482) om elektronisk kommunikation (LEK) om undantag från tillhandahållarnas skyldighet att utplåna och avidentifiera trafikuppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande (prop. 2020/21:72 s. 30 och 72). Regleringen finns numera i 9 kap. LEK. Bestämmelserna i LEK om lagring av uppgifter, när lagrade uppgifter får behandlas och när bevarade uppgifter inte får utplånas gjordes även tillämpliga i fall där uppgifter har bevarats med stöd av 27 kap. 16 § RB (prop. 2020/21:72 s. 72 f.).

Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § LEK och bevarar uppgifter på grund av ett föreläggande enligt 27 kap. 16 § RB ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de bevarade uppgifterna och ska enligt 9 kap. 29 b § LEK bedriva verksamheten så att uppgifterna utan dröjsmål kan lämnas ut (prop. 2020/21:72 s. 73).

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till en viss uppgift ska, enligt 9 kap. 33 § första stycket 5 LEK även lämna ut uppgifter om vilka övriga tillhandahållare som har deltagit vid överföringen av det meddelande som omfattas av föreläggandet (prop. 2020/21:72 s. 75 f.).

Tystnadsplikt

Även bestämmelserna om tystnadsplikt för tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster gjordes tillämpliga på uppgifter som hänför sig till ett föreläggande enligt 27 kap. 16 § RB (prop. 2020/21:72 s. 74).

7.2.4 Genomförandet av artikel 29

Ömsesidig rättslig hjälp ska enligt artikel 29 kunna lämnas med ett sådant skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter som avses i artikel 16. För att genomföra artikel 29 ändrades 1 kap. 2 § 6 och 2 kap. 1 och 2 §§ lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) och en ny paragraf, 4 kap. 24 c §, infördes i den lagen. Regleringen innebär bl.a. att rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § RB ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång och enligt de särskilda bestämmelserna i LIRB (prop. 2020/21:72 s. 32 f. och 71 f.).

Vidare ändrades 1 kap. 4 § 4 lagen (2017:1000) om en europeisk utredningsorder så att en utredningsorder ska kunna avse ett föreläggande enligt 27 kap. 16 § RB.

7.2.5 Sveriges tillträde till det andra tilläggsprotokollet

E-bevisutredningens betänkande

E-bevisutredningen lämnade den 20 december 2024 betänkandet Effektivare gränsöverskridande inhämtning av elektroniska bevis (SOU 2024:85). Utredningen hade bl.a. i uppdrag att se över regleringen om gränsöverskridande tillgång till elektroniska bevis med anledning av det andra tilläggsprotokollet till Budapestkonventionen. Betänkandet, som har remissbehandlats, bereds i Regeringskansliet.

Det andra tilläggsprotokollet syftar, som tidigare nämnts, till att ytterligare stärka samarbetet vid utredning av it-brottslighet och insamling av bevis i elektronisk form i samband med brottsutredningar

eller straffrättsliga förfaranden. Utredningen föreslår att Sverige ska tillträda det andra tilläggsprotokollet (SOU 2024:85 s. 342).

För att genomföra det andra tilläggsprotokollet i svensk rätt föreslår utredningen att åklagare och övriga brottsbekämpande myndigheter ska ha rätt att från en registreringsenhet för toppdomäner eller återförsäljare av domännamn respektive från en tjänsteleverantör i en annan stat som tillträtt det andra tilläggsprotokollet dels begära uppgifter för att identifiera eller kontakta innehavaren av ett domännamn, dels begära uppgifter om abonnemang som skäligen kan antas ha betydelse för utredningen om ett brott.

Vidare föreslår utredningen att en registreringsenhet för toppdomäner eller återförsäljare av domännamn, som erbjuder tjänster för domännamnsregistrering i Sverige, på begäran till en behörig myndighet i en annan stat, som tillträtt det andra tilläggsprotokollet, ska lämna ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn om uppgifterna rör brottslig verksamhet eller misstanke om brott.

Utredningen föreslår även att Sverige ska lämna en förklaring i vilken Sverige förbehåller sig att artikel 8, om verkställighet av order från en annan part avseende skyndsamt framtagande av abonnemangsuppgifter och trafikuppgifter, endast tillämpas på de brott och brottstyper som avses i 27 kap. 19 a § andra stycket och 19 b § andra stycket RB. Vidare föreslås att Sverige bör förbehålla sig rätten att inte tillämpa artikel 8 vad avser insamling av trafikuppgifter inom en tjänsteleverantörs datasystem som dels drivs för en sluten användargrupp, dels inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datasystem.

7.3 Utvärdering av Budapestkonventionen

Utvärderingen av artikel 19.2 i Budapestkonventionen

Artikel 19 i Budapestkonventionen reglerar husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter. Enligt punkten 1 ska medlemsstaterna vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att genom husrannsakan eller på liknande sätt inom territoriet bereda sig tillgång till

a) ett datasystem eller en del därav och de datorbehandlingsbara uppgifter som lagras däri, och

b) ett medium för lagring av datorbehandlingsbara uppgifter i vilket uppgifter kan vara lagrade.

Medlemsstaterna ska enligt punkten 2 vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att se till att myndigheterna, när de genom husrannsakan eller på liknande sätt bereder sig tillgång till ett visst datasystem eller en del därav enligt punkt 1 a och har anledning att tro att de eftersökta uppgifterna är lagrade i ett annat datasystem eller en del av ett annat datasystem inom dess territorium och sådana uppgifter är lagligen åtkomliga eller tillgängliga för det första systemet, skyndsamt ska kunna utvidga husrannsakan eller det liknande sättet till att bereda sig tillgång till detta andra system.

Artikel 19 har utvärderats i en rapport som antogs i december 2024 och som bygger på den fjärde utvärderingsrundan bland konventionens medlemsstater. Syftet med utvärderingen är att samla erfarenheter och praxis kring hur olika länder har genomfört artikel 19 i nationell rätt och i praktiskt polisiärt arbete. Utvärderingen syftar också att ge rekommendationer för framtida reformer och stärkt internationellt samarbete mot cyberbrott.

I utvärderingen drogs en mycket allmän slutsats i rapporten att vissa parters nationella lagstiftning ställer krav på att det anslutna datasystemet ska finnas inom den stats territorium som verkställer åtgärden, medan andra parters nationella lagstiftning inte ställer ett sådant krav. Det verkar dock som att många parter kan utöka sin tillgång till uppgifter om uppgifterna eventuellt finns i en annan jurisdiktion, förutsatt att uppgifterna är tillgängliga från den partens territorium. Vissa stater skulle, om de inte hade något annat val, medvetet utvidga sökandet till ett annat land under vissa omständigheter. De omständigheterna kan vara mycket begränsade (Cybercrime Convention Committee [T-CY], Assessing Article 19 Budapest Convention on the search and seizure of stored computer data: Assessment Report adopted by the 31st Plenary of the T-CY on 12 December 2024, s. 95 f.).

7.4 Den praktiska tillämpningen

Enligt Åklagarmyndighetens statistik utfärdade åklagare 68 föreläggande enligt 27 kap. 16 § RB under år 2024. Regleringen tillämpas framför allt på begäran av annan stat.

8 Cybersäkerhet

8.1 EU-lagstiftning om cybersäkerhet

8.1.1 NIS 2-direktivet och CER-direktivet

EU antog år 2022 ett direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå inom EU (NIS 2-direktivet).[1] I syfte att bl.a. genomföra direktivet i svensk rätt har det införts en cybersäkerhetslag (2025:1506), med tillhörande förordning (2025:1507), som trädde i kraft den 15 januari 2026. Den nya lagen innebär att offentliga och enskilda verksamhetsutövare inom vissa utpekade sektorer bl.a. ska vidta åtgärder för att skydda sina nätverks- och informationssystem och rapportera betydande incidenter. Den nya lagen innehåller också regler om tillsyn och ingripandemöjligheter mot verksamhetsutövare som inte följer regleringen. Samtidigt gjordes, med anledning av CER-direktivet,[2] ändringar i andra lagar som rör elektronisk kommunikation, toppdomäner och sekretess.

8.1.2 Cyberresiliensförordningen

EU:s cyberresiliensförordning,[3] som trädde i kraft den 10 december 2024 men i huvudsak ska tillämpas från den 11 december 2027, syftar till att skapa förutsättningar för utvecklingen av säkra produkter med digitala element, genom att säkra att hårdvaru- och program-

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.
[2] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet).
[3] Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828.

varuprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Förordningen syftar också till att skapa förutsättningar för att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder. Cyberresiliensförordningen gäller för produkter inom olika sektorer, bl.a. konsumentelektronik, industriell automation och it-säkerhetslösningar. Den är tillämplig på exempelvis smartphones, datorer, nätverkskomponenter och programvara för säkerhet. Vissa kategorier av produkter definieras som viktiga eller kritiska, vilket innebär skärpta krav och i vissa fall att produkten blir föremål för tredjepartsbedömning eller certifiering. Viktiga produkter är bl.a. lösenordshanterare, operativsystem, routrar, brandväggar och smarta hemprodukter med säkerhetsfunktioner. Kritiska produkter är hårdvaruenheter med säkerhetsboxar, smarta mätarportar inom smarta mätarsystem och smartkort eller liknande enheter. Ekonomiska operatörer, i huvudsak tillverkare, importörer och distributörer, ska följa de cybersäkerhetskrav som förordningen anger för alla produkter med digitala element, för att de ska få tillhandahållas på den inre marknaden. Kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och vid utvecklingen av produkter med digitala element. Vidare ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, vara transparenta gentemot konsumenter gällande cybersäkerhetsaspekter och tillförsäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt under produktens hela livscykel.

8.1.3 Kompletterande bestämmelser till cyberresiliensförordningen

I betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115) föreslås de kompletterande bestämmelser som behövs för att anpassa svensk rätt till förordningen. Utredningen föreslår att en ny lag, lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning, införs och en ny förordning. I lagen anges att regeringen får utse anmälande myndighet och marknadskontrollmyndighet. I lagen finns även bestämmelser om marknadskontrollmyndigheternas befogenheter och möjlighet att besluta om sanktioner, även mot myndigheter, för överträdelser av

regelverket. Några straffrättsliga bestämmelser föreslås inte, däremot andra typer av sanktioner. Betänkandet har remissbehandlats och bereds i Regeringskansliet.

8.2 Arbetet för att säkerställa cybersäkerhet

8.2.1 Nationell strategi för cybersäkerhet

Regeringen har tagit fram Nationell strategi för cybersäkerhet 2025, skr. 2024/25:121. Strategin beskriver regeringens inriktning för arbetet med frågor av betydelse för Sveriges cybersäkerhet. Den utgår från nationella behov och från NIS 2-direktivet och dess allriskperspektiv för att hantera en bredd av utmaningar. I strategin beskrivs ett antal hot och sårbarheter som påverkar Sveriges cybersäkerhet. Strategin utgår från följande tre pelare som anger inriktningen för Sveriges cybersäkerhetsarbete

- systematiskt och effektivt cybersäkerhetsarbete,
- utvecklad kunskap och kompetensutveckling inom cybersäkerhet, och
- förmåga att förhindra och hantera cybersäkerhetsincidenter.

Strategin innehåller bl.a. mål som tar sikte på ett antal områden för att bemöta de hot och sårbarheter som redovisas i strategin. Till strategin kopplas en handlingsplan, som ska uppdateras löpande.

Regeringen har också publicerat skriften En ny era av cybersäkerhet, Nationell strategi för cybersäkerhet 2025–2029. Strategin och den tillhörande handlingsplanen har utarbetats med bistånd av aktörer i både offentlig och privat sektor. Strategin kommer regelbundet, minst vart femte år, att utvärderas på grundval av strategins resultatindikatorer i enlighet med NIS 2-direktivets krav.

8.2.2 En ny organisation för att möta aktuella hot

Nationellt center för cybersäkerhet

Nationellt center för cybersäkerhet (NCSC) startade år 2020. Från den 1 november 2024 är NCSC en del av Försvarets radioanstalt enligt 4 § förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

NCSC har till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter enligt 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt.

Vidare ska NCSC utgöra en nationell plattform för samverkan och informationsutbyte mellan aktörer, såväl privata som offentliga, i frågor som rör cybersäkerhet. Centret ska också vara en kontaktpunkt för sådana frågor.

Enligt 3 § förordningen om det nationella cybersäkerhetscentret vid Försvarets radioanstalt ska NCSC särskilt

1. bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet,
2. lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet,
3. lämna råd och stöd till privata och offentliga aktörer vid it-incidenter,
4. genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet,
5. till privata och offentliga aktörer ta fram samlade lägesbilder av antagonistiska cyberhot och andra it-incidenter,
6. bistå Regeringskansliet (Försvarsdepartementet) med samlade lägesbilder som bl.a. innehåller bedömningar av hotnivån,
7. vara en kontaktpunkt gentemot motsvarande funktioner i internationella sammanhang och utveckla samarbetet och informationsutbytet med dessa,
8. rapportera till regeringen om förhållanden på cybersäkerhetsområdet som kan leda till behov av åtgärder samt lämna förslag på sådana åtgärder, och

9. informera regeringen om relevanta förhållanden vid ett sådant hot eller annan incident som är av mindre allvarligt slag.

Försvarets radioanstalt ska i den verksamhet som bedrivs inom ramen för NCSC samverka med Försvarets materielverk, Försvarsmakten, Myndigheten för civilt försvar, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen (4 och 5 §§ förordningen om det nationella cybersäkerhetscentret vid Försvarets radioanstalt).

En grundläggande förutsättning för att man inom NCSC ska kunna bedriva ett effektivt arbete är att Försvarets radioanstalt och samverkansmyndigheterna kan utbyta nödvändig information med varandra. Eftersom den nuvarande sekretessregleringen innebär att det saknas förutsättningar för ett ändamålsenligt informationsutbyte och det är ett hinder för sådan samverkan som krävs för att stärka cybersäkerheten har det bl.a. föreslagits en ny lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret. Lagen träder i kraft den 15 juli 2026 (Lagändringar för ett stärkt nationellt cybersäkerhetscenter, prop. 2025/26:214, s. 5 och 13 f.).

Computer Emergency Response Team

Computer Emergency Response Team (CERT-SE) är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja det svenska samhället i arbetet med att hantera och förebygga it-säkerhetsincidenter (se Informationssäkerhet för samhällsviktiga och digitala tjänster, prop. 2017/18:205, s. 77 f.). Uppdraget omfattar både privat och offentlig sektor med fokus på samhällsviktig verksamhet. CERT-SE är en del av Myndigheten för civilt försvar. Till uppdraget hör bl.a. att

- agera skyndsamt vid inträffade it-säkerhetsincidenter genom att sprida information och stödja verksamheter i arbetet med att avhjälpa eller lindra effekter av det inträffade,
- ta emot incidentrapporter och samordna insatser vid större it-säkerhetsincidenter,
- tillhandahålla risk- och incidentanalyser och lägesuppfattning beträffande cybersäkerhet,

- delta i CSIRT-nätverket, och
- vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder och att utveckla samarbetet och informationsutbytet med dem.

8.2.3 Säkerhetspolisens arbete mot hot mot cybersäkerheten

Allmänt om läget och aktuella hot

Säkerhetspolisen har en nyckelroll när det gäller att upptäcka och förhindra hot mot cybersäkerheten från främmande makt. Beskrivningen i det följande är i huvudsak hämtad från Säkerhetspolisens offentliga redovisning av verksamheten under åren 2024–2026.

Cyberangrepp har blivit ett viktigt verktyg för främmande makt. Det används både mot enskilda personer och för att bygga upp anonymiseringsnätverk för att genomföra angrepp där den bakomliggande aktören är svår eller omöjlig att knyta till angreppet. Sveriges säkerhet påverkas av en orolig omvärld och det allvarliga säkerhetsläget kan komma att försämras ytterligare. Det handlar både om främmande makts agerande och ett fortsatt högt terrorhot och om fortsatta brister i säkerheten kring skyddsvärda svenska verksamheter som utnyttjas av hotaktörer. Under senare år har ett flertal händelser ägt rum som har fått stor medial uppmärksamhet och som ibland har beskrivits som s.k. hybridhot. Det är bl.a. cyberangrepp, drönarflygningar och kabelbrott i Östersjön. Hybrida aktiviteter genomförs ofta med hjälp av ombud, för att dölja den bakomliggande aktören. Säkerhetspolisen bedriver i nationell och internationell samverkan en omfattande verksamhet för att bedöma och utreda händelserna.

Cyberangrepp som verktyg

Genom riktade cyberangrepp kan främmande makt få tillgång till information om Sveriges säkerhet, om politiskt beslutsfattande eller annan information som kan användas i kartläggnings- eller påverkanssyfte. Måltavlor för angreppen kan vara myndigheter, men även enskilda personer som beslutsfattare eller oppositionella. Angripare kan vara såväl främmande makt som andra aktörer, t.ex. kriminella

grupperingar, som gör det för ekonomisk vinning. Informationen kan användas för kartläggning av sårbarheter eller för att försöka påverka samhällsutvecklingen. Främmande makt har också intresse av privatpersoners enheter, t.ex. mobiltelefoner eller datorer, för riktad inhämtning eller för att bygga anonymiseringsnätverk för fortsatta angrepp eller i påverkanssyfte. Cyberangrepp kan även användas för att skaffa eftertraktad kunskap och teknik. Säkerhetspolisen känner till att utländska cyberhotaktörer har genomfört angrepp mot bl.a. svenska försvars- och teknikföretag.

Vissa utländska säkerhets- och underrättelsetjänster har hög förmåga att inhämta underrättelseinformation digitalt och de har alla egna enheter som genomför cyberangrepp. Säkerhetspolisen pekar särskilt på Ryssland, Kina och Iran. De ryska och kinesiska säkerhets- och underrättelsetjänsterna riktar sig mot en mängd olika politiska, militära och ekonomiska mål i Sverige medan Iran ofta fokuserar på oppositionella i diasporan. I dag är tröskeln för att genomföra cyberangrepp mot mål i Sverige låg, eftersom det finns betydande sårbarheter som kan utnyttjas. Omfattande sårbarheter i svensk infrastruktur och svenska it-system, kombinerat med främmande makts höga förmåga att agera i digital miljö och stora informationsbehov, utgör därför enligt Säkerhetspolisen ett allvarligt hot mot Sveriges säkerhet.

Iranska säkerhets- och underrättelsetjänster har genomfört cyberangrepp mot enskilda individer, i första hand oppositionella, i Sverige genom att göra intrång i individers mobiltelefoner och datorer genom att installera skadlig kod i dem i syfte att kartlägga deras förehavanden och kontakter. För att styra den skadliga koden som installerats på enheterna utnyttjas servrar runt om i världen som kontrolleras av den iranska regimen. Säkerhetspolisen har utrett flera ärenden där den iranska underrättelsetjänsten har genomfört intrång och sedan hämtat information från de berörda enheterna.

Även kinesiska säkerhets- och underrättelsetjänster gör intrång i privatpersoners enheter, främst i syfte att bygga upp större anonymiseringsnätverk för att kunna agera förnekbart. Genom sådana nätverk kan de sedan genomföra cyberangrepp mot bl.a. myndigheter och institutioner och samtidigt dölja den bakomliggande aktörens trafik och identitet. Säkerhetspolisen har tidigare uppmärksammat hur kinesisk underrättelsetjänst har gjort intrång i tiotusentals privatpersoners servrar och routrar i Sverige, i syfte att bygga upp en egen

digital infrastruktur. Den används sedan för att angripa andra länder och deras myndighetsfunktioner från svensk mark. Säkerhetspolisen har även utrett ärenden där kinesisk underrättelsetjänst har riktat cyberangrepp mot mål i Sverige.

Irans säkerhets- och underrättelsetjänster arbetar långsiktigt utifrån sina målsättningar men kan även agera opportunistiskt om tillfälle uppstår. I samband med koranbränningarna i Sverige under sommaren 2023 gjorde en iransk cyberaktör intrång i ett svenskt företags datasystem för att skicka ut massmeddelanden. Genom att etablera och ta kontroll över företagets system skickade den iranska cyberaktören ut sms till tusentals personer över hela Sverige med uppmaning att lämna information om dem som utförde koranbränningar. Angreppet var omfattande och Säkerhetspolisen har kunnat fastslå att det iranska revolutionsgardet låg bakom operationen, som bedöms ha varit en påverkanskampanj mot Sverige. Säkerhetspolisen bedömde att kampanjen genomfördes i syfte att stärka den iranska regimen genom att måla upp bilden av Sverige som ett islamfientligt land och skapa splittring i det svenska samhället.

Främmande makt har intresse av att genom cyberangrepp få tillgång till information som berör svensk säkerhet, politiska beslut eller annan myndighetsutövning. Det kan medföra att myndigheter och politiska beslutsfattare blir måltavlor för angreppen. Främmande makt kan använda informationen för att kartlägga sårbarheter eller för att försöka påverka beslut men också för att destabilisera och skapa oro. Cyberangrepp utförs även av aktörer som främst drivs av ekonomiska eller ideologiska skäl och som saknar koppling till främmande makt.

De senaste årens teknikutveckling har inneburit mer lättillgängliga metoder och ökad förmåga hos aktörer att genomföra cyberangrepp. Angripare använder ofta kända tekniska sårbarheter som det kan finnas skydd mot, men där användarna inte har gjort nödvändiga säkerhetsuppdateringar. Avancerade angripare har också förmåga att identifiera mindre kända eller helt okända sårbarheter att utnyttja för angrepp. Säkerhetspolisen har sett många it-incidenter som orsakats genom brister i grundläggande cybersäkerhet.

8.2.4 Polismyndighetens verksamhet

Polismyndighetens uppdrag är att upprätthålla allmän ordning och säkerhet och ingripa mot alla typer av brott, utom de brott som ligger inom Säkerhetspolisens verksamhetsområde. Polismyndighetens arbete har genom det ett annat fokus. Myndighetens verksamhet har de senaste åren i hög grad präglats av effekterna av crime as a service, särskilt det förhållandet att rekryteringen online har lett till att många ungdomar har förmåtts att utföra mord och sprängningar.

It-brottscentrum vid nationella operativa avdelningen (NOA) vid Polismyndigheten är en nationell expertresurs som skapar förutsättningar för enhetlighet vid uppklaring och utredning av it-relaterade brott. It-brottscentrum ansvarar för kontakterna med Europol i frågor om cyberbrottslighet. Det är de nationella polismyndigheterna som i praktiken utför polisarbetet, eftersom Europols roll enbart är att agera samordnare och kunskapscentrum.

8.2.5 EU:s arbete mot hot mot cybersäkerheten

Europols övergripande roll

Europol har till uppgift att stödja medlemsstaterna i EU i arbetet att förebygga och bekämpa alla former av allvarlig internationell och organiserad brottslighet, cyberbrott och terrorism. Europol samarbetar också med många partnerländer utanför EU och med internationella organisationer. Enligt Europol utgör storskaliga kriminella nätverk och terroristnätverk ett betydande hot mot EU:s inre säkerhet och mot EU:s befolknings säkerhet och försörjning. Enligt en av de senaste hotbildsbedömningarna avseende internetorganiserad brottslighet blir brottsligheten alltmer aggressiv och konfrontativ.

Cyberbrott är alltså ett växande problem för EU:s medlemsstater, där internetinfrastrukturen i de flesta länder är välutvecklad och betalningssystemen är online. Det är dock inte bara finansiella uppgifter som är ett viktigt mål för cyberbrott, utan även uppgifter i allmänhet. Antalet och frekvensen av dataintrång ökar, vilket i sin tur leder till fler fall av bedrägeri och utpressning.

Cyberbrott har varit en av EU:s prioriteringar i kampen mot grov och organiserad brottslighet som en del av European Multidiscipli-

nary Platform Against Criminal Threats (Empact) under åren 2022–2025. Empact är en EU-plattform som riktar in sig på brottslingar som iscensätter cyberangrepp, särskilt de som erbjuder specialiserade brottstjänster online. Arbetet inom Empact består bl.a. i att sammanställa hotbildsbedömningar och att utarbeta operativa handlingsplaner.

År 2010 inrättade Europol tillsammans med Europeiska kommissionen och EU:s medlemsstater Europeiska unionens arbetsgrupp mot it-brottslighet (EUCTF), ett förtroendebaserat nätverk vars roll är att identifiera, diskutera och prioritera de viktigaste utmaningarna och åtgärderna i kampen mot it-brott.

Europol är en viktig partner i det internationella nätverket för att förebygga it-brott, InterCOP, som består av totalt 26 länder. InterCOP-nätverket syftar till att koppla samman brottsbekämpande myndigheter för att dela expertis och gemensamt utveckla, genomföra och utvärdera initiativ för att förebygga cyberbrott.

Europeiska cyberbrottscentrumet

Med hänsyn till bredden av cyberangrepp inrättade Europol år 2013 Europeiska cyberbrottscentrumet (The European Cybercrime Centre, EC3) för att stärka insatserna mot cyberbrott inom EU. På operativ nivå fokuserar EC3 på cyberbrott som är beroende av internet, cyberbrott i form av sexuell exploatering av barn och internetbedrägeri. EC3 erbjuder operativt, strategiskt, analytiskt och kriminaltekniskt stöd till medlemsstaternas utredningar avseende sådana cyberbrott. EC3 fungerar som ett nav för information och underrättelser om sådana brott. EC3 tillhandahåller specialiserad teknisk och digital kriminalteknisk stödkapacitet för utredningar och operationer och en mängd olika strategiska analysprodukter som underlättar för medlemsstaterna att bekämpa och förebygga cyberbrott. EC3 har också en uppsökande funktion som kopplar samman brottsbekämpande myndigheter med den privata sektorn, den akademiska världen och andra icke-brottsbekämpande partners. Det stöd som ges innefattar stöd för att bekämpa brott på Darknet och alternativa plattformar.

EC3 har en tredelad strategi för kampen mot cyberbrottslighet som utgörs av expertis och intressenthantering, forensisk undersökning och operationer.

EC3 arbetar för att se till att alla partners kan spela en roll i den gemensamma kampen mot cyberbrottslighet. Centrumet har därför inrättat en säker plattform för ackrediterade experter på cyberbrottslighet, där experter kan utbyta praxis och ytterligare utöka kunskapsbasen om sådan brottslighet.

EC3 är också värd för Joint Cybercrime Action Taskforce. Dess uppdrag är att driva på underrättelsestyrda och samordnade operationer mot viktiga hot i form av cyberbrott, bl.a. brott i form av sexuell exploatering av barn och internetbedrägeri och måltavlor som främjar cyberbrottslighet (t.ex. brottslig användning av Darknet). Det görs genom gemensam identifiering, prioritering, förberedelse, inledande och genomförande av gränsöverskridande brottsutredningar och operationer med hjälp av partners.

Varje år offentliggör EC3 sin hotbildsbedömning avseende internetbaserad brottslighet, som fastställer prioriteringar för Empacts operativa handlingsplan för den brottslighet som står i fokus för det året. Rapporten innehåller en brottsbekämpningsinriktad bedömning av de framväxande hoten och redovisar den viktigaste utvecklingen på cyberbrottsområdet under det senaste året.

It-brottscentrum vid NOA ansvarar, som nyss nämnts, för kontakterna med och hanteringen och samordningen av underrättelser inom EC3 och utgör dess svenska motsvarighet – Swedish Cyber Crime Center (SC3), se Polisens tillgång till information om vissa it-incidenter, Ds 2016:22, s. 63 f.

9 Något om brottsutvecklingen

9.1 Bakgrund

Som tidigare nämnts är ett typiskt kännetecken för cyberbrottslighet att den ofta är gränsöverskridande. För att kunna bekämpa sådan brottslighet effektivt krävs det därmed i många fall internationellt samarbete. Av det skälet arbetar både Europol och Eurojust aktivt med frågor som rör den sortens brottslighet.

9.2 Årliga rapporter från Europol

Europol redovisar varje år en rapport om hur organiserad brottslighet i digital miljö utvecklas, vilka hot den kan innebära och vilka utmaningar de brottsbekämpande myndigheterna står inför. I de tre senaste rapporterna har Europol redovisat dels aktuella brottstrender (IOCTA 2024),[1] dels hur kriminella säljer och utnyttjar persondata som är tillgängliga på internet (IOCTA 2025),[2] dels hur cyberbrottsligheten har industrialiserats genom artificiell intelligens (AI), kryptering och anonymiseringsstrukturer (IOCTA 2026)[3].

I rapporten från år 2024 anges de huvudsakliga cyberhoten vara följande.

- Den ständigt växande volymen av material som rör sexuella övergrepp mot barn.

[1] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, Luxembourg.
[2] Europol, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment (IOCTA) 2025, Publications Office of the European Union, Luxembourg.
[3] Europol, The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026, Publications Office of the European Union, Luxembourg, 2026.

- Investeringsbedrägerier, bedrägerier via företags e-post och romansbedrägerier. Nätfiske är fortfarande den vanligaste formen av angrepp vid bedrägerier.
- Digital skimming som leder till stöld och vidareförsäljning eller missbruk av kreditkortsuppgifter.
- Att verktyg och tjänster baserade på AI används i allt större utsträckning.
- Att ransomwareangrepp i allt större utsträckning riktas mot små och medelstora företag, eftersom de har sämre cyberförsvar.

Vidare pekas på att användningen av Darknet, kryptovalutor och olika applikationer med totalsträckskryptering bidrar till att underlätta för kriminella att begå brott. TOR-nätverket uppges fortfarande vara det vanligaste sättet att komma åt Darknet.

I fråga om sexuella övergrepp mot barn är ett ihållande hot fall där förövare tittar på sexuella övergrepp mot barn på begäran, med hjälp av en eller flera personer som utför övergreppen på barnen i utbyte mot betalning. Det är den huvudsakliga formen av kommersiellt sexuellt utnyttjande av barn och en viktig källa till nytt övergreppsmaterial.

I rapporten från år 2025 framhålls att stöld av data är ett betydande hot. Persondata är mycket värdefull för en mängd olika kriminella aktörer som utnyttjar den som en handelsvara i sig, men också som ett mål för andra syften, inklusive annan kriminell verksamhet. Kriminella använder en mängd olika tekniker för att stjäla personuppgifter och utnyttjar både sårbarheter i systemen och bristande mänsklig kontroll. Teknikerna används av olika kriminella aktörer som ofta kombinerar dem i olika skeden av den kriminella processen. Social manipulering utmärker sig som en särskilt vanlig teknik.

Den framväxande användningen av AI i kriminella affärsmodeller har enligt rapporten lagt till ett nytt lager av komplexitet i hotbilden. Kriminella kan använda AI bl.a. för angreppsautomation, social manipulering och att kringgå säkerhetsåtgärder. Information kan också användas i AI-aktiverade angrepp, t.ex. för att göra förfalskningar, skapa syntetiska medier och skapa falska identiteter.

I rapporten redovisas ingående hur det har byggts upp en särskild organisation som hanterar, köper och säljer stulen data. Kriminella kan köpa olika typer av data som de utnyttjar eller de verktyg och

tjänster som används för att förvärva dem, via olika plattformar huvudsakligen baserade på Darknet. Exempel på det som bjuds ut till försäljning är följande.

- Icke analyserade loggar från verktyg för att stjäla information och läckt eller stulen data, som kan innehålla bl.a. personuppgifter och användaruppgifter för olika tjänster.
- Icke analyserade eller verifierade kreditkortsdumpar (vanligtvis insamlade genom digital skimming) och bulkförsäljning av verifierade kortuppgifter.
- Erbjudanden om initiala åtkomstuppgifter, allt från autentiseringsuppgifter för fjärrtjänster och konton (t.ex. VPN, brandväggar, nätverksenheter och molnmiljöer) till etablerad bakdörrsåtkomst till företagssystem och nätverk.
- Kontoinloggningsuppgifter för olika webbtjänster, inklusive bl.a. e-post- och sociala mediekonton och online-shoppingmiljöer.
- Kriminella tjänster, inklusive prenumerationer på verktyg som används för att utnyttja sårbarheter i programvara, operativsystem och förfalskningstjänster.
- Lösningar mot upptäckt, t.ex. VPN, penningtvättstjänster och manualer för driftsäkerhet.

Även ”vishing”, dvs. användningen av bedrägliga telefonsamtal som lurar måltavlor att lämna ut känslig information, möjliggörs av förekomsten av förfalskningstjänster. Sådana tjänster gör det möjligt för kriminella att utge sig för att vara lokala och välrenommerade enheter som passar måltavlorna, vilket ökar effektiviteten i social manipulation. Tekniken används i stor utsträckning för att utföra bedrägerier och för att få initial tillgång till system.

Rapporten från år 2026 framhåller hur cyberbrottsligheten har blivit alltmer industrialiserad, organiserad och tekniskt avancerad. Cyberbrott utförs inte i lika stor utsträckning som tidigare av enskilda personer, utan av kriminella nätverk som agerar i en struktur som går att jämföra med professionella företag med egna tjänster, leveranskedjor och internationella samarbeten. Rapporten beskriver hur AI, krypterade kommunikationstjänster, kryptovalutor och crime as a service-modeller har förändrat den digitala brottsmiljön.

En central del av rapporten rör de verktyg och infrastrukturer som möjliggör cyberbrott och förändrar strukturen och omfattningen av cyberbrottsligheten. Europol beskriver hur marknadsplatser på Darknet fortsätter att existera trots återkommande insatser från polisen. När en plattform stängs ner flyttar användarna snabbt till nya tjänster. Krypterade meddelandeapplikationer och anonymiseringstjänster gör det svårare för myndigheter att spåra kriminella aktiviteter. De som begår brott i cybermiljö använder bl.a. proxyservrar och hyrd digital infrastruktur för att dölja sina identiteter och skydda sin verksamhet från upptäckt.

Europol varnar för att generativa AI-verktyg används för att skapa övertygande phishing-mail, falska webbplatser, deepfake-videor och automatiserade bedrägerier. AI gör det möjligt att genomföra angrepp i mycket större skala och med högre kvalitet än tidigare. Även personer med begränsad teknisk kunskap kan med hjälp av AI skriva skadlig kod, översätta texter, analysera stulen information eller genomföra avancerad social manipulation.

9.3 Eurojusts och Europols gemensamma rapport

Rapporten Gemensamma utmaningar inom cyberbrottslighet[4] är ett samarbete mellan Eurojust och Europol som behandlar både existerande och framväxande utmaningar med cyberbrott och utredningar som involverar digitala bevis. Rapporten innehåller uppdateringar om utvecklingen inom cyberbrott och diskuterar ny lagstiftning som syftar till att öka effektiviteten för att bekämpa cyberbrott.

Rapporten belyser flera nya EU-instrument. De har utformats för att hantera den ökande datamängden, de pågående problemen med förlust av tillgången till data och utmaningar som anonymiseringstjänster medför i samband med brottsutredning och åtal. Syftet med EU-instrumenten är att effektivisera processer och göra det enklare för behöriga myndigheter som arbetar med brottsutredningar och åtal att hantera stora datamängder och effektivisera internationellt samarbete.

Vidare identifieras i rapporten viktiga utmaningar beträffande cyberbrott. En sådan är datahantering, vilket kräver att brottsbekäm-

[4] Eurojust and Europol (2025), Common Challenges in Cybercrime – 2024 review by Eurojust and Europol, Publication Office of the European Union, Luxembourg.

pande myndigheter hanterar enorma datamängder. Det skapar behov av avancerade analystekniker och betydande resurser som för närvarande ligger utom räckhåll för många myndigheter. Dessutom skapar teknik som döljer användaridentiteter och platser eller som blockerar laglig tillgång till data betydande hinder för att spåra olaglig verksamhet. Internationellt samarbete möter också rättsliga och logistiska hinder som komplicerar kampen mot cyberbrott, som ofta sträcker sig över flera jurisdiktioner. Vidare stöter samarbete mellan offentliga och privata partners, som kan vara avgörande för att lösa cyberbrott, ofta på hinder bl.a. i form av begränsningar för datadelning och sekretess för brottsutredningarna.

Rapporten beskriver Eurojusts och Europols gemensamma strategiska inriktningar i kampen mot cyberbrottslighet.

Något som rapporten särskilt pekar på är att dataförlust utgör en särskild utmaning i utredningar av cyberbrott. EU-domstolens ogiltigförklaring av datalagringsdirektivet[5] har skapat osäkerhet i hela Europa i fråga om vad som gäller för datalagring för brottsbekämpande ändamål. Det är oklart om, och i så fall vilka typer av data, som ska lagras av tjänsteleverantörer och hur länge de ska lagras. Eftersom det för närvarande inte finns någon standardiserad EU-rättslig ram för datalagring för brottsbekämpande ändamål, finns det i vissa EU-medlemsstater ingen datalagringsperiod alls, medan uppgifterna i andra medlemsstater lagras endast i några få dagar. Det innebär i vissa fall att dataförfrågningar når tjänsteleverantörerna efter det att datalagringsperioden har löpt ut och att det därmed inte finns någon möjlighet att fortsätta brottsutredningen.

Vidare lyfts problemet med anonymiseringstjänster. Det är enligt rapporten ofta svårt att fastställa den fysiska platsen för kriminella och deras verksamhet. Det är också ofta oklart var deras uppgifter lagras. Även när det kan fastställas, leder det ibland till flera jurisdiktioner som är svåra att nå för brottsbekämpande myndigheter eller rättsväsendet. Länder har traditionellt förlitat sig på ömsesidig rättslig hjälp och den europeiska utredningsordern för att få tillgång till elektroniska bevis från andra jurisdiktioner. De rättsliga instrumenten orsakar dock ofta långa förseningar i utredningar. Data i cyberbrottsutredningar kan flyttas från ett datacenter till ett annat på

[5] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

sekunder, medan det kan ta månader att få svar i förfaranden för ömsesidig rättslig hjälp eller utredningsorder.

Datalagring på internet blir mer decentraliserad. Decentraliseringen är ytterligare en utmaning för brottsbekämpande myndigheter och rättsväsendet. Kriminella tjänster, bl.a. marknadsplatser på Darknet, lagras ofta på virtuella privata servrar. Data som lagras på molnbaserade tjänster kan enkelt flyttas eller skickas till datacenter i andra länder. Data kan också speglas, vilket skapar förutsättningar för flera versioner av samma server eller säkerhetskopior. De kriminella kan använda sådana kopior om lokala myndigheter stänger ner verksamheten. Dessutom uppstår rättslig osäkerhet kring databeslag, eftersom bevis tenderar att vara utspridda över flera jurisdiktioner när de lagras på olika molntjänster.

En annan relaterad fråga är distribuerad lagring. Nya lagringsmetoder gör det omöjligt för brottsbekämpande myndigheter att skicka en begäran till en webbhotelleverantör om att ta bort olagligt innehåll. Det kan leda till teknisk oförmåga att ta bort t.ex. material från sexuella övergrepp mot barn, terrorismrelaterat innehåll och annat olagligt innehåll. Därför måste nya tekniska och rättsliga metoder för att hantera distribuerade nätverk utvecklas.

9.4 Särskilt om crime as a service

Fenomenet crime as a service, som har skapat en sorts ”tjänstemarknad” för brott, är relativt nytt. I Sverige kännetecknas verksamheten framför allt av att genomförande av mycket grova brott, bl.a. sprängningar och skjutningar, ”annonseras” på vissa digitala plattformar. Ofta lockas den som genomför brotten med en hög ekonomisk ersättning för att begå brott. Olika kriminella nätverk står bakom verksamheten. De personer som agerar rekryterare finns ofta utomlands och gömmer sig normalt under olika alias. I stor utsträckning är det barn och unga som rekryteras online.

Enligt Polismyndigheten anstiftades och koordinerades sprängoch skjutvapenvåldet i Sverige under åren 2024 och 2025 i många fall i den digitala miljön (Ds 2026:1 s. 14). Utvecklingen tyder på att crime as a service i allt större utsträckning används även vid andra typer av brott och likaså i Säkerhetspolisens verksamhetsområde.

10 En internationell utblick

10.1 Bakgrund

Utredningen har i uppdrag att kartlägga och redovisa andra jämförbara länders rättsliga möjligheter att störa, sabotera och avbryta pågående brottslighet i cybermiljö.

Redogörelsen görs i huvudsak mot bakgrund av de länders lagstiftning som de brottsbekämpande myndigheterna har hänvisat till i sina behovsbeskrivningar i kapitel 11, dvs. Australien, Belgien, Danmark, Estland, Finland, Frankrike, Nederländerna, Storbritannien och Tyskland. Redogörelsen syftar till att ge en övergripande bild över utländsk lagstiftning som rör olika former av ingripanden i digital miljö i såväl underrättelseverksamhet som brottsutredning.

Det kan i sammanhanget konstateras att den svenska rättsordningen skiljer sig från flera andra länders rättsordningar där polis och åklagare har organiserats på annat sätt än i Sverige. Den svenska regleringen vilar på grundprincipen om obligatorisk åtalsplikt och objektivitetskrav för åklagare.

10.2 Sammanfattning

Den utländska lagstiftning som redovisas i detta kapitel ger i de flesta fall brottsbekämpande myndigheter befogenheter att ingripa i digital miljö på sätt som i huvudsak motsvarar bestämmelserna om genomsökning på distans eller hemlig dataavläsning enligt svensk rätt i det avseendet att det är tillåtet att bereda sig tillgång till informationssystem och ta del av uppgifter i dem. I en del fall finns det även möjlighet att blockera eller stänga ner hemsidor. Enligt de flesta länders lagstiftning fattas beslut om sådana ingripanden av domstol, åklagare eller s.k. undersökningsdomare. I några fall fattar politiska befatt-

ningshavare sådana beslut. Polisen har dock enligt flera länders lagstiftning befogenheter att fatta interimistiska beslut. Det kan vara såväl på underrättelsestadiet som i brottsutredning. Förutsättningarna är i flera fall att det ska finnas någon grad av misstanke om brott. Det finns dock i flera fall inte något krav på att det ska finnas någon misstänkt person utan endast ett identifierbart informationssystem. Vidare finns det flera bestämmelser i den utländska lagstiftningen som ger uttryck för att proportionalitetsprincipen ska beaktas. Det finns också i viss lagstiftning befogenheter för brottsbekämpande myndigheter att skaffa sig tillträde till platser i samband med ett ingripande. I flertalet fall finns det bestämmelser där journalister och några andra yrkeskategorier under vissa förutsättningar undantas från brottsbekämpande myndigheters befogenheter att ingripa i digital miljö.

Den mest långtgående lagstiftningen inom cyberområdet finns i Australien. Lagstiftningen ger brottsbekämpande myndigheter befogenheter att under vissa förutsättningar vidta åtgärder som ändrar, stör eller raderar uppgifter i datasystem. Åtgärderna får riktas mot datasystem för att bl.a. förhindra och avbryta brott och förutsätter inte att det finns någon misstänkt person. Enligt den australienska lagstiftningen fattar domstol beslut som gäller i 90 dagar och besluten får förlängas eller återkallas. Lagstiftningen är tillfällig och utvärderas för närvarande. Det går därför enligt utredningens mening inte att dra några säkra slutsatser om lagstiftningens genomslag i tillämpningen.

10.3 Regleringen i Australien

10.3.1 Allmänt om regleringen

I Surveillance Devices Act 2004 regleras statliga och territoriella brottsbekämpande myndigheters användning av övervakningsanordningar. Den omfattar

- dataövervakningsanordningar – enheter eller program som används på datorer,
- avlyssningsanordningar – enheter som används för att lyssna på eller spela in samtal,

- optiska övervakningsanordningar – enheter som används för att spela in bilder eller observera aktiviteter, och
- spårningsanordningar – enheter som används för att lokalisera eller spåra en person eller ett föremål.

Surveillance Devices Act innehåller inga förbud mot användning av övervakningsanordningar, utan de regleras i lagstiftning som gäller i de australiska delstaterna och territorierna. Undantag gäller dock vid utredning av statliga och territoriella brott. Surveillance Devices Act kompletterar lagstiftning om övervakningsanordningar som gäller i de australiska delstaterna och territorierna genom att den tillåter övervakning i syfte att utreda federala brott och statliga brott med federala inslag.

The Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 införde tre nya befogenheter för den australiska federala polisen (Australian Federal Police, ”AFP”) och den australiensiska brottskommissionen (Australian Crime Commission, ”ACC”[1]) i syfte att kunna identifiera och störa allvarlig brottslig verksamhet online.

- Tillstånd till dataavbrott – som tillåter att datatrafik avbryts genom modifiering och radering av data för att hindra att allvarliga brott begås, t.ex. distribution av material som innehåller övergrepp mot barn.
- Tillstånd till nätverksaktivitet – som möjliggör insamling av underrättelser om allvarlig brottslig verksamhet som begås av kriminella nätverk som verkar online.
- Tillstånd till att överta kontrollen över ett onlinekonto – som tillåter att kontrollen över en persons onlinekonto övertas för att samla in bevis i syfte att utreda brott.

Bestämmelserna om tillstånd till dataavbrott och tillstånd till nätverksaktivitet har införts i del 2 i Surveillance Devices Act.

Bestämmelserna om tillstånd till att överta kontrollen över ett onlinekonto har införts i del I i Crimes Act 1914. Crimes Act är en federal lag som innehåller bestämmelser om brott som begås mot Australien och om straffprocessuella tvångsmedel.

[1] Numera ”Australian Criminal Intelligence Commission” (ACIC).

10.3.2 Dataavbrott och nätverksaktivitet

Tillstånd till dataavbrott

Bestämmelserna om tillstånd till dataavbrott (”data disruption warrants”) gäller under fem år från och med att de har trätt i kraft.

En brottsbekämpande tjänsteman vid AFP eller ACC, får hos domstol ansöka om ett tillstånd till dataavbrott om tjänstemannen på rimliga grunder misstänker att

a) ett eller flera brott har begåtts, håller på att begås, kommer att begås, eller sannolikt kommer att begås,

b) brotten involverar, eller sannolikt kommer att involvera, data som lagras i en dator (måldatorn), och

c) åtgärden sannolikt väsentligt kommer att bidra till att motverka att det misstänkta brottet eller brotten begås genom att datan involverar, eller sannolikt kommer att involvera, data som lagras i måldatorn.

Med måldator i punkten b) avses en viss dator, en dator i en viss lokal, eller en dator som är förknippad med, används av eller sannolikt kommer att användas av en person, vars identitet kan vara känd eller okänd.

Domstol får besluta om tillstånd till dataavbrott om det finns rimliga skäl för den misstanke om brott som ligger till grund för ansökan om åtgärden och åtgärden är berättigad och proportionerlig. Vid den bedömningen ska bl.a. beaktas

a) arten och allvaret i det misstänkta brottet eller brotten[2],

b) i vilken utsträckning åtgärden kommer att bidra till att hindra att det misstänkta brottet eller brotten begås,

c) förekomsten av alternativa åtgärder för att hindra att det misstänkta brottet eller brotten begås,

d) i vilken utsträckning verkställandet av åtgärden sannolikt kommer att resultera i tillgång till, eller störning av, uppgifter som rör personer som lagligen använder datorn, och eventuella integri-

[2] Det rör sig bl.a. om brott mot rikets säkerhet eller brott mot person med en straffskala på fängelse i tre år eller mer eller annars brott som är av gränsöverskridande eller allvarlig karaktär eller som utgör organiserad brottslighet.

tetskonsekvenser (i den mån de är kända) som följer av tillgången eller störningen,

e) eventuella åtgärder som föreslås för att undvika eller minimera den omfattning i vilken verkställandet av åtgärden sannolikt kommer att påverka personer som lagligen använder datorn,

f) i vilken utsträckning verkställandet av åtgärden sannolikt kommer att orsaka en person tillfällig förlust av

   i) pengar,

   ii) digital valuta, eller

   iii) egendom (annan än data),

g) om bl.a.

   i) domstolen på rimliga grunder anser att datan som omfattas av åtgärden rör en person som yrkesmässigt arbetar som journalist eller en arbetsgivare till en sådan person,

   ii) det misstänkta brottet, eller vart och ett av de misstänkta brotten, utgör brott mot en sekretessbestämmelse, och

h) eventuella tidigare begärda eller beslutade tillstånd avseende samma misstänkta brott.

Ett tillstånd till åtgärden ska bl.a. innehålla uppgifter om

a) de omständigheter som tillståndet grundar sig på,

b) de misstänkta brotten,

c) den tid under vilket tillståndet gäller (som längst 90 dagar),

d) de villkor under vilka åtgärden får vidtas, och

e) den dator som åtgärden riktar sig mot, den lokal eller det fordon som datorn finns i och den person som datorn används av (antingen genom namn eller på annat sätt).

Ett tillstånd ger följande befogenheter – i förhållande till de villkor som anges i beslutet om tillstånd – avseende en måldator

a) att tillträda en lokal i syfte att få tillträde till eller lämna de specificerade lokalerna,

b) att använda
   i) måldatorn,

   ii) en telekommunikationsanläggning som drivs eller tillhandahålls av staten eller en operatör,

   iii) någon annan elektronisk utrustning, eller

   iv) en datalagringsenhet,

   i syfte att

   i) få tillgång till relevanta data som lagras i måldatorn när som helst medan beslutet är i kraft, för att avgöra om datan omfattas av tillståndet,

   ii) störa datan när som helst medan beslutet om tillstånd är i kraft, om det sannolikt bidrar till att förhindra att det misstänkta brottet eller brotten begås,

c) att lägga till, kopiera, radera eller ändra andra data i måldatorn om det är nödvändigt för att uppnå det syfte som anges i punkten b),

d) om det, med beaktande av andra metoder, som sannolikt är lika effektiva, är rimligt under samtliga omständigheter, för att få tillgång till data eller störa data

   i) använda någon annan dator eller kommunikation under överföring, och

   ii) lägga till, kopiera, radera eller ändra andra data i datorn eller kommunikationen under överföring,

e) att avlägsna en dator eller annan egendom från lokaler i syfte att göra något som anges i tillståndet och återställa datorn eller annan egendom, och

f) att avlyssna kommunikation som passerar över ett telekommunikationssystem, om avlyssningen görs i syfte att utföra någon åtgärd som anges i tillståndet.

Åtgärden får inte innebära att tillägga, radera eller ändra data eller en handling som sannolikt

a) väsentligt stör, avbryter eller hindrar:

   i) en kommunikation under överföring, eller

ii) andra personers lagliga användning av en dator,

om inte åtgärden är nödvändig och proportionerlig för att vidta de åtgärder som anges i tillståndet, eller

b) orsakar någon annan väsentlig förlust eller skada för andra personer som lagligen använder en dator, såvida inte förlusten eller skadan är skäligen nödvändig och proportionerlig för att göra en eller flera av de åtgärder som anges i tillståndet.

I brådskande fall får en behörig auktoriserad tjänsteman, efter ansökan av en brottsbekämpande tjänsteman vid AFP eller ACC, besluta om tillstånd till dataavbrott. Det gäller om den brottsbekämpande tjänstemannen under en utredning av ett misstänkt brott har rimliga skäl att tro bl.a. att det finns en överhängande risk för allvarligt våld mot en person eller betydande skada på egendom, åtgärden är nödvändig för att hantera risken och det inte finns några alternativa, mindre ingripande, åtgärder för att hantera risken. Beslutsfattaren ska inom 48 timmar, efter beslutet, ansöka hos domstol om godkännande av tillståndet.

Verkställighet m.m.

Ett tillstånd till dataavbrott tillåter användning av våld mot personer och egendom som är nödvändig och rimlig för att utföra de åtgärder som anges i tillståndet.

Domstol får, efter ansökan av en brottsbekämpande tjänsteman, besluta dels om förlängning av tillståndet med som längst 90 dagar efter att tillståndet löper ut, dels om ändring av villkoren för tillståndet.

Domstol får vidare besluta att återkalla ett tillstånd. Om ett tillstånd inte längre behövs ska, förutom att tillståndet ska återkallas, den brottsbekämpande myndigheten vidta nödvändiga åtgärder för att säkerställa att tillgången till och avbrottet av data upphör.

Tillstånd till nätverksaktivitet

Bestämmelserna om tillstånd till nätverksaktivitet (“network activity warrants”) gäller under fem år från och med att de har trätt i kraft.

Chefen för AFP eller ACC får hos domstol, ansöka om ett tillstånd till nätverksaktivitet om chefen på rimliga grunder misstänker att

a) en grupp individer är ett kriminellt nätverk av individer[3],

b) tillgång till data som lagras i en dator (måldatorn), som används, eller sannolikt kommer att användas, av någon av individerna i gruppen, väsentligt kommer att bidra till insamling av underrättelser som

   i) avser gruppen eller någon av individerna i gruppen, och

   ii) är relevanta för att förebygga, upptäcka eller förhindra att ett eller flera misstänkta brott begås.

Vid tillämpning av punkten a) är det oväsentligt om identiteten på individerna i gruppen kan fastställas, om det sannolikt kommer att ske förändringar i gruppens sammansättning eller om måldatorn eller dess plats kan identifieras.

Med måldator i punkten b) avses en dator som används, eller sannolikt kommer att användas, av en person, vars identitet kan vara känd eller okänd, och antingen är en viss dator eller en dator som då och då befinner sig i en viss lokal.

Domstol får besluta om tillstånd till nätverksaktivitet om det finns rimliga grunder för misstanke om brott som ligger till grund för ansökan och åtgärden är berättigad och proportionerlig. Vid den bedömningen ska följande beaktas

a) arten och allvaret i det misstänkta brottet eller brotten i relation till den information som kan erhållas med anledning av åtgärden,

[3] Med ett kriminellt nätverk av individer avses en elektroniskt sammanlänkad grupp av individer under vissa närmare angivna förutsättningar. Med en elektroniskt sammanlänkad grupp av individer avses en grupp av två eller fler individer där varje individ i gruppen använder, eller sannolikt kommer att: a) använda samma elektroniska tjänst som minst en annan individ i gruppen och/eller b) kommunicerar med minst en annan individ i gruppen genom elektronisk kommunikation.

b) i vilken utsträckning tillgång till uppgifter enligt tillståndet kommer att bidra till insamling av underrättelser som

   i) avser en grupp eller någon av individerna i gruppen, och

   ii) är relevant för att förebygga, upptäcka eller förhindra att det misstänkta brottet eller brotten begås,

c) det sannolika underrättelsevärdet av den information som åtgärden kommer att generera,

d) om åtgärderna i tillståndet står i proportion till det sannolika underrättelsevärdet av den information som åtgärden kommer att generera,

e) alternativa eller mindre ingripande sätt att erhålla den information som åtgärden kommer att generera,

f) i vilken utsträckning åtgärden sannolikt kommer att resultera i tillgång till uppgifter för personer som lagligen använder datorn, och eventuella integritetskonsekvenser, i den mån de är kända, som följer av tillgången,

g) om bl.a.

   i) domstolen på rimliga grunder anser att varje målkonto innehas av en person som yrkesmässigt arbetar som journalist eller av en arbetsgivare till en sådan person,

   ii) det misstänkta brottet, eller vart och ett av de misstänkta brotten, utgör brott mot en sekretessbestämmelse, och

h) eventuella tidigare begärda eller beslutade tillstånd avseende samma misstänkta brott.

Ett tillstånd till åtgärden ska bl.a. innehålla uppgifter om

a) de omständigheter som tillståndet grundar sig på,

b) de misstänkta brotten,

c) det kriminella nätverk av individer som tillståndet avser,

d) den tid under vilket tillståndet gäller (som längst 90 dagar),

e) de villkor under vilka åtgärden får vidtas, och

f) huruvida åtgärden ska vidtas i kombination med någon övervakningsutrustning, vilken utrustning som i sådant fall avses och syftet med användningen av utrustningen.

Ett tillstånd ger följande befogenheter – i förhållande till de villkor som anges i tillståndet – avseende en måldator

a) att tillträda specificerade lokaler i syfte att utföra de åtgärder som tillståndet avser,

b) att tillträda lokaler i syfte att få tillträde till eller lämna de specificerade lokalerna,

c) att använda

i) måldatorn,

ii) en telekommunikationsanläggning som drivs eller tillhandahålls av staten eller en operatör,

iii) någon annan elektronisk utrustning, eller

iv) en datalagringsenhet,

i syfte att få tillgång till relevanta data som lagras i måldatorn när som helst medan tillståndet gäller för att avgöra om datan omfattas av tillståndet,

d) att lägga till, kopiera, radera eller ändra andra data i måldatorn om det är nödvändigt för att uppnå det syfte som anges i punkten c),

e) om det, med beaktande av andra metoder, som sannolikt är lika effektiva, är rimligt under samtliga omständigheter, för att få tillgång till data

i) använda någon annan dator eller kommunikation under överföring, och

ii) lägga till, kopiera, radera eller ändra andra data i datorn eller kommunikationen under överföring,

f) att avlägsna en dator eller annan egendom från lokalen i syfte att göra något som anges i tillståndet och återställa datorn eller annan egendom,

g) att avlyssna kommunikation som passerar i ett telekommunikationssystem, om avlyssningen görs i syfte att utföra någon åtgärd som anges i tillståndet, och

h) att använda en övervakningsanordning i syfte att utföra någon åtgärd som anges i tillståndet.

Åtgärden får inte innebära att tillägga, radera eller ändra data eller en handling som sannolikt

a) väsentligt stör, avbryter eller hindrar

   i) en kommunikation under överföring, eller

   ii) andra personers lagliga användning av en dator, om inte tillägget, raderingen eller ändringen av data eller handlingen är nödvändig för att göra en eller flera av de åtgärder som anges i tillståndet, eller

b) orsakar någon annan väsentlig förlust eller skada för andra personer som lagligen använder datorn.

Verkställighet m.m.

Ett tillstånd till nätverksaktivitet tillåter användning av det våld mot personer och egendom som är nödvändigt och rimligt för att utföra de åtgärder som anges i tillståndet.

Domstol får efter ansökan besluta dels om förlängning av tillståndet med som längst 90 dagar efter att tillståndet löper ut, dels om ändring av villkoren för tillståndet.

Domstol får vidare besluta om att återkalla ett tillstånd. Om ett tillstånd inte längre behövs ska, förutom att tillståndet ska återkallas, den brottsbekämpande myndigheten vidta nödvändiga åtgärder för att säkerställa att tillgången till data upphör.

Internationell anknytning

Om det, innan ett tillstånd till dataavbrott eller ett brådskande tillstånd till dataavbrott beslutas eller ett tillstånd till nätverksaktivitet beslutas, blir uppenbart för sökanden att det kommer att finnas be-

hov av tillgång till eller avbrott av data som lagras i en dator i ett annat land eller på ett fartyg eller på ett flygplan som är registrerat enligt ett annat lands lag och som befinner sig i eller ovanför vatten utanför Australiens territorialhavs yttre gränser, får domstol endast bevilja tillstånd till åtgärden om tillgången eller avbrottet har godkänts av en behörig tjänsteman i det andra landet.

Om ett tillstånd till dataavbrott eller nätverksaktivitet redan har beslutats, anses tillståndet omfatta tillgång till data respektive avbrott av data endast om åtgärden har godkänts av en behörig tjänsteman i det andra landet.

Hänvisningen till en behörig tjänsteman i det främmande landet ska även anses vara en hänvisning till en behörig tjänsteman i varje berört främmande land.

Det som nu sagts gäller inte bl.a. om

a) den person, eller var och en av de personer som ansvarar för att verkställa åtgärden, kommer att vara fysiskt närvarande i Australien och platsen där data lagras är okänd eller rimligen inte kan fastställas,

b) ett fartyg, som är registrerat enligt ett främmande lands lag, finns i vatten utanför Australiens territorialhavs yttre gränser, men inte utanför Australiens angränsande zons yttre gränser, och det misstänkta brottet utgör ett brott som rör Australiens tull-, skatte-, immigrations- eller hälsovårdslagstiftning eller andra särskilt angivna brott, om fartyget finns utanför Australiens territorialhavs yttre gränser, men inte utanför Australiens fiskezons yttre gränser.

10.3.3 Övertagande av kontrollen över ett onlinekonto

Tillstånd till att överta kontrollen över ett onlinekonto

Bestämmelserna om tillstånd till att överta kontrollen över onlinekonton (”account takeover warrants”) gäller under fem år från och med att de har trätt i kraft.

Med tillstånd till att överta kontrollen över ett onlinekonto avses att en person vidtar ett eller flera steg som resulterar i att personen har en exklusiv tillgång till onlinekontot genom att t.ex. använda befintliga kontouppgifter för att ändra en eller flera kontouppgifter, ta bort ett krav på tvåfaktorsautentisering eller ändra den eller de typer

av kontouppgifter som krävs för att komma åt eller använda kontot. Med ett onlinekonto avses ett konto som en elektronisk tjänst har för en slutanvändare.

En brottsbekämpande tjänsteman får ansöka om tillstånd till åtgärden om tjänstemannen har rimliga skäl att tro att

a) ett eller flera brott har begåtts, håller på att begås, kommer att begås, eller sannolikt kommer att begås,

b) en utredning om brotten pågår, kommer att pågå, eller sannolikt kommer att pågå, och

c) åtgärden är nödvändig under utredningen i syfte att inhämta bevis för att brottet eller brotten har begåtts.

Domstol får besluta om tillstånd till åtgärden om det finns rimliga grunder för misstanken om brott som ligger till grund för ansökan. Vid den bedömningen ska följande beaktas

a) arten och allvaret i det misstänkta brottet eller brotten[4],

b) förekomsten av alternativa sätt att erhålla bevisning,

c) i vilken utsträckning någon persons integritet sannolikt kommer att påverkas,

d) det sannolika bevisvärdet av den information som kommer att erhållas genom åtgärden,

e) i vilken utsträckning verkställandet av åtgärden sannolikt kommer att påverka personer som lagligen använder en dator,

f) i vilken utsträckning verkställandet av åtgärden sannolikt kommer att orsaka en person tillfällig förlust av

   i) pengar,

   ii) digital valuta, eller

   iii) egendom (annan än data),

g) om bl.a.

[4] Det rör sig bl.a. om brott mot rikets säkerhet eller brott mot person med en straffskala på fängelse i tre år eller mer eller andra brott som är av gränsöverskridande eller allvarlig karaktär eller som utgör organiserad brottslighet.

i) domstolen på rimliga grunder anser att varje målkonto innehas av en person som yrkesmässigt arbetar som journalist eller av en arbetsgivare till en sådan person,

ii) det misstänkta brottet, eller vart och ett av de misstänkta brotten, utgör brott mot en sekretessbestämmelse,

h) tidigare begärda eller beslutade tillstånd avseende samma onlinekonto, och

i) tidigare begärda eller beslutade tillstånd avseende samma misstänkta brott.

Ett beslut om tillstånd till åtgärden ska bl.a. innehålla uppgifter om

a) de omständigheter som tillståndet grundar sig på,

b) det misstänkta brottet eller brotten,

c) den tid under vilket tillståndet gäller (som längst 90 dagar),

d) de onlinekonton som tillståndet avser,

e) innehavarna och användarna av onlinekontona, såvitt de är kända, och

f) de villkor under vilka åtgärden får vidtas.

Ett tillstånd ger följande befogenheter – i förhållande till de villkor som anges i tillståndet – avseende varje målkonto

a) att ta kontroll över målkontot när som helst medan tillståndet gäller i syfte att möjliggöra bevisinhämtning avseende det misstänkta brottet eller brotten,

b) att, i syfte att ta kontroll över målkontot, använda

i) en dator,

ii) en telekommunikationsanläggning som drivs eller tillhandahålls av staten eller en operatör,

iii) annan elektronisk utrustning, eller

iv) en datalagringsenhet.

c) om det är nödvändigt för att ta kontroll över målkontot

i) tillgång till kontobaserade uppgifter som avser målkontot,

ii) att lägga till, kopiera, radera eller ändra kontouppgifter som avser målkontot, eller

iii) att lägga till, kopiera, radera eller ändra data i en dator.

Vid tillämpning av bestämmelsen omfattas kontobaserade uppgifter av ett tillstånd under förutsättning att tillgången till uppgifterna är nödvändiga i utredningen för att hämta in bevisning avseende det misstänkta brottet eller brotten.

Åtgärden får inte innebära att tillägga, radera eller ändra data eller en handling som sannolikt

a) väsentligt stör, avbryter eller hindrar

i) en kommunikation under överföring, eller

ii) andra personers lagliga användning av en dator, om inte tillägget, raderingen eller ändringen av data eller handlingen är nödvändig för att göra en eller flera av de åtgärder som anges i tillståndet, eller

b) orsakar någon annan väsentlig förlust eller skada för andra personer som lagligen använder en dator.

I brådskande fall får en behörig auktoriserad tjänsteman, efter ansökan av en brottsbekämpande tjänsteman, besluta om tillstånd till att överta kontrollen över ett onlinekonto om den brottsbekämpande tjänstemannen under en utredning av ett eller flera misstänkta brott har rimliga skäl att tro bl.a. att det föreligger en överhängande risk för allvarligt våld mot en person eller betydande skada på egendom, åtgärden är nödvändig för att hantera risken och det inte finns några alternativa mindre ingripande åtgärder för att hantera risken. Beslutsfattaren ska inom 48 timmar efter beslutet ansöka hos domstol om godkännande av tillståndet.

Verkställighet m.m.

Ett tillstånd till kontoövertagande får inte verkställas på ett sätt som leder till förlust eller skada på data, om inte skadan är berättigad och proportionerlig med hänsyn till det misstänkta brottet eller brotten

eller orsakar en person en permanent förlust av pengar, digital valuta eller egendom (förutom data).

Domstol får efter ansökan besluta dels om förlängning av tillståndet med som längst 90 dagar efter att tillståndet löper ut, dels om ändring av villkoren för tillståndet.

Domstol får besluta att återkalla ett tillstånd. Åtgärden ska avbrytas om den inte längre är nödvändig för att hämta in bevisning avseende det misstänkta brottet eller brotten. Nödvändiga åtgärder ska vidtas för att säkerställa att verkställigheten avbryts.

Den information som erhållits med anledning av tillstånd till att överta kontrollen av ett onlinekonto måste förvaras så att den inte är tillgänglig för personer som inte har rätt att hantera den. Informationen ska förstöras så snart som möjligt om materialet inte längre behövs, och senast inom fem år. Vidare finns det bestämmelser om regelbunden rapportering om tillstånden och tillsyn över verkställigheten av tillstånden.

10.4 Regleringen i Belgien

10.4.1 Åtgärder i brottsutredande syfte

Husrannsakan i datasystem

Enligt den belgiska straffprocesslagen (”Code d’instruction criminelle”) får s.k. husrannsakan i ett datasystem eller en del av ett sådant system, som består i att kopiera, göra data oåtkomlig och att radera data som lagrats i ett datasystem eller en del därav, genomföras.

En husrannsakan i ett datasystem eller en del av ett sådant system som har tagits i beslag eller som kan komma att beslagtas får beslutas av en tjänsteman vid kriminalpolisen eller, efter att ett sådant ärende hänskjutits till åklagare, av åklagare. När det gäller vissa typer av brottsutredningar ska beslut fattas av undersökningsdomare. I sådana fall ska åtgärden vara nödvändig för att utreda brottet och andra åtgärder vara oproportionerliga eller så ska det finnas risk för att bevis går förlorade om åtgärden inte genomförs.

Utan samtycke från ägaren eller användaren av ett datasystem, får åklagare eller undersökningsdomare när som helst besluta om tillfälligt avlägsnande av allt skydd från datasystemet. Det får vid behov göras med hjälp av tekniska medel, falska signaler, falska nycklar

eller falska egenskaper eller installation av tekniska anordningar i datasystemet för att dekryptera och avkoda data som lagras, bearbetas eller överförs av systemet.

Åklagaren eller undersökningsdomaren ska så snart som möjligt underrätta den person som ansvarar för datasystemet om att husrannsakan i datasystemet har ägt rum.

Åklagaren ska använda lämpliga tekniska medel för att garantera uppgifternas integritet och konfidentialitet och för att bevara dem.

Avlyssning och andra åtgärder i datasystem

En undersökningsdomare får besluta att meddelanden som inte är tillgängliga för allmänheten eller data i ett datasystem eller en del av ett sådant, med hjälp av tekniska medel, i hemlighet får avlyssnas, ges tillgång till, utforskas eller spelas in.

En sådan åtgärd får endast beslutas i undantagsfall, när utredningen kräver det, om det finns allvarliga indikationer på att det rör sig om ett i lagen särskilt angivet fullbordat brott eller försök till sådant brott och om andra utredningsmetoder inte är tillräckliga för att utreda brottet.

För att möjliggöra en sådan åtgärd får undersökningsdomaren även, utan den boendes, ägarens eller användarens vetskap eller samtycke, när som helst besluta om

a) tillträde till en bostad, en privat lokal eller ett datasystem,

b) tillfälligt avlägsnande av skydd för ett datasystem, med hjälp av tekniska medel, falska signaler, falska nycklar eller falska inloggningsuppgifter, och

c) installation av tekniska anordningar i ett datasystem i syfte att dekryptera och avkoda data som lagras, bearbetas eller överförs av det systemet.

Åtgärden får endast beslutas för att söka efter uppgifter som kan användas för att utreda brott. Den får endast riktas mot personer som misstänks ha begått brottet, eller med avseende på de kommunikationsmedel eller datasystem som regelbundet används av en misstänkt, eller med avseende på de platser som den misstänkte för-

modas besöka. Åtgärden får även riktas mot personer som kan antas stå i regelbunden kommunikation med en misstänkt.

En åklagare får besluta om åtgärden under förutsättning att en gärningsman grips på bar gärning och brottet avser vissa i lagen särskilt angivna brott. Ett sådant beslut ska fattas inom 72 timmar efter det att brottet upptäcktes.

I beslut om åtgärden ska bl.a. anges den person, det kommunikationsmedel, det datasystem eller den plats som är föremål för åtgärden och den tidsperiod under vilken åtgärden får genomföras, vilken inte får överstiga en månad.

De tjänstemän som verkställer åtgärden ska minst var femte dag skriftligen rapportera om verkställigheten till undersökningsdomaren.

En undersökningsdomare får förlänga ett tillstånd med längst en månad, dock totalt längst sex månader. Så snart de omständigheter som motiverar åtgärden inte längre föreligger ska tillståndet upphävas.

De tjänstemän som verkställer åtgärden ska ge undersökningsdomaren tillgång till bl.a. de uppgifter från datasystemet som erhållits och platsen för de uppgifter som avses i datasystemet samt en allmän beskrivning av innehållet i och identifieringsuppgifterna för datasystemet med avseende på data som anses irrelevanta.

Lämpliga metoder ska användas för att säkerställa integriteten och konfidentialiteten för icke-offentliga tillgängliga meddelanden eller data. Det finns också bestämmelser som reglerar hur uppgifterna i ett datasystem ska hanteras efter att en åtgärd genomförts.

Vidare regleras registrering, förvaring och förstörande av uppgifter i ett datasystem och en tilltalads och dennes ombuds rätt att, på begäran, få en kopia av uppgifter i ett datasystem som med anledning av dess relevans har registrerats i en rapport som de har rätt att ta del av. Det föreskrivs även skyldighet att årligen rapportera uppgifter om användningen av åtgärderna till parlamentet.

En behörig utländsk myndighet kan under vissa förutsättningar ges tillstånd att avlyssna eller på annat sätt ta del av uppgifter i datasystem om det föreskrivs i ett för Belgien bindande internationellt instrument.

10.4.2 Åtgärder i underrättelseverksamhet

Allmänt

I lagen om underrättelsetjänster (loi organique des services de renseignement et de sécurité) från år 2018 finns bestämmelser som reglerar både den civila underrättelse- och säkerhetstjänstens och den militära underrättelse- och säkerhetstjänstens underrättelsemetoder. Metoderna får inte användas i syfte att kränka eller bryta mot individuella fri- och rättigheter. Vidare ska subsidiaritets- och proportionalitetsprinciperna beaktas vid underrättelseinsamling. Som huvudregel får inte underrättelse- och säkerhetstjänsterna förvärva, analysera eller använda uppgifter som skyddas av antingen advokatsekretess eller läkares tystnadsplikt eller sekretess för journalistiska källor.

Underrättelse- och säkerhetstjänsterna får, i syfte att fullgöra sina uppdrag, oberoende av om tekniska resurser, falska signaler, falska nycklar eller falsk kapacitet används

a) skaffa tillgång till ett datasystem,

b) neutralisera eventuella säkerheter som systemet kan ha,

c) använda tekniska förfaranden för att dechiffrera och avkoda de uppgifter som lagras, behandlas eller överförs av datasystemet, och

d) kopiera data som lagras, bearbetas eller överförs av datasystemet.

När det gäller statliga myndigheters datasystem får åtgärden endast vidtas efter förhandsgodkännande från den berörda statliga myndigheten.

Vidare får åtgärden endast ha till syfte att samla in relevanta underrättelser som lagras, behandlas eller överförs av datasystemet, utan att det medför någon oåterkallelig radering eller ändring av uppgifterna i det.

Underrättelse- och säkerhetstjänsterna får när som helst, utan ägarens eller dennes rättighetsinnehavares vetskap eller samtycke, bereda sig tillträde till platser som inte är tillgängliga för allmänheten och få tillgång till låsta eller olåsta föremål för att

a) bereda sig tillgång till datasystem,

b) installera en teknisk anordning där, använda den eller avlägsna den, och

c) avlägsna datasystemen och återställa dem.

Den tekniska anordningen eller datasystemet ska återställas eller bytas ut så snart som möjligt efter intrånget, såvida det inte skulle hindra ett korrekt utförande av underrättelse- och säkerhetstjänsternas uppdrag.

Underrättelse- och säkerhetstjänsterna får för att kunna utföra sina uppdrag fånga in, lyssna på och spela in kommunikation, utan ägarens eller dennes rättighetsinnehavares vetskap eller samtycke, genom att bereda sig tillträde till platser för att

a) installera en teknisk anordning där, använda den eller avlägsna den,

b) öppna ett låst föremål för att placera en teknisk anordning i det, och

c) avlägsna föremålet för att installera en teknisk anordning i det, manövrera föremålet och därefter återställa det.

Den tekniska anordningen eller det borttagna föremålet ska återställas eller bytas ut så snart som möjligt efter avlyssningen, om det inte skulle hindra ett korrekt utförande av uppdraget.

Om det krävs ett ingripande i ett elektroniskt kommunikationsnät ska chefen för avdelningen skicka en skriftlig begäran till nätoperatören eller leverantören av en elektronisk kommunikationstjänst, som sedan är skyldig att tillhandahålla tekniskt samarbete.

Åtgärderna får endast vidtas om det finns ett allvarligt potentiellt hot mot rikets grundläggande intressen i vissa närmare angivna avseenden och om andra mindre ingripande metoder är otillräckliga.

En avdelningschef vid underrättelsetjänsten ska ta fram ett förslag till åtgärd till en särskild kommission, som utövar tillsyn över åtgärderna.

En åtgärd får som huvudregel pågå under två månader. Åtgärden ska upphöra om det allvarliga potentiella hot som motiverade åtgärden har upphört, när metoden inte längre tjänar det syfte för vilket den beslutades eller om metoden är olaglig.

I avdelningschefens förslag till åtgärd ska bl.a. anges

a) den typ av åtgärd som avses,

b) de fysiska eller juridiska personer, sammanslutningar eller grupper, föremål, platser, händelser eller den information som är föremål för åtgärden,

c) det allvarliga potentiella hot som motiverar åtgärden,

d) de faktiska omständigheter som motiverar åtgärden och skälen för att åtgärden är förenlig med subsidiaritetsprincipen och proportionalitetsprincipen,

e) den tidsperiod som åtgärden ska gälla,

f) överlappningen med en brottsutredning eller rättslig utredning, och

g) de brott som berörs.

Kommissionen ska ge sitt samtycke inom fyra dagar efter mottagandet av förslaget, annars får åtgärden inte verkställas. En behörig minister får då godkänna åtgärden. Om åtgärden är synnerligen brådskande kan ministern bevilja åtgärden, som i sådant fall får pågå högst fem dagar. Under vissa omständigheter får den pågå en längre tidsperiod.

10.4.3 Åtgärd vid vissa allvarliga cyberangrepp

Den civila underrättelse- och säkerhetstjänsten får enligt en särskild bestämmelse bereda sig tillgång till ett datasystem som finns utomlands, inaktivera dess säkerhetsdetaljer, använda tekniska förfaranden på det för att dechiffrera, avkoda, spara och manipulera de uppgifter som lagras, behandlas eller vidarebefordras av datasystemet och störa och neutralisera datasystemet. Det får endast göras i syfte att samla in, analysera och behandla underrättelser som bl.a. rör nationell och internationell säkerhet och verksamheter som kan hota rikets intressen i vissa närmare angivna avseenden. Det får vidare endast göras i syfte att, i samband med cyberangrepp mot vapensystem, militära dator- och kommunikationssystem eller system som förvaltas av försvarsministern, neutralisera angreppet och identifiera förövaren, utan att det påverkar rätten att omedelbart svara med ett eget cyberangrepp i enlighet med bestämmelser i lagstiftning som rör väpnade konflikter.

Ett sådant ingrepp i datasystem ska föregås av en granskning som ska utföras på grundval av årligen upprättade förteckningar över de organisationer eller institutioner som kommer att bli föremål för ingrepp i sina datasystem under det kommande året med en motivering till intrånget och den förväntade varaktigheten. Förteckningarna ska godkännas av försvarsministern. Om ett ingrepp i ett datasystem visar sig vara väsentligt och brådskande för att fullgöra underrättelse- och säkerhetstjänstens uppdrag, får intrånget genomföras utan försvarsministerns godkännande. Försvarsministern ska i sådant fall så snart som möjligt, och senast den första arbetsdagen efter det att operationen inleddes, underrättas. Försvarsministern kan besluta att åtgärderna ska upphöra.

Det finns även bestämmelser om kontroll av pågående ingrepp i datasystem och granskning av sådana intrång efter att de har verkställts.

En ständig kommitté har bl.a. rätt att stoppa olagliga ingrepp i datasystem och kan besluta att de uppgifter som har erhållits på ett olagligt sätt inte får användas och att de ska förstöras.

10.5 Regleringen i Danmark

10.5.1 Blockering av webbplats

Enligt § 791 d rettsplejeloven får en webbplats blockeras om det finns en saklig grund att anta att webbplatsen bryter mot vissa i lagen särskilt angivna brott[5].

När bestämmelsen infördes anfördes i förarbetena att det då endast var tekniskt möjligt att blockera en hel webbplats med hjälp av en s.k. DNS-blockering, även om endast en liten del av innehållet på webbplatsen utgjorde ett brott. Vidare anfördes att det exempelvis inte var möjligt att blockera en profil på ett socialt medium utan endast hela det sociala mediet, vilket i allmänhet fick antas vara ett oproportionerligt ingrepp. I de fall där det olagliga materialet på en webbplats endast utgör en liten del kan polisen ändå kontakta t.ex. den som administrerar webbplatsen för att uppmärksamma det faktum att sidan – enligt polisens bedömning och eventuellt även enligt

[5] Det gäller även vissa andra brott än de som omfattas av TCO-förordningen.

hyresgästens egna riktlinjer – innehåller olagligt material (2016/1 LSF 192 s. 19 och 49).

Beslut om tillstånd till blockering fattas av domstol efter ansökan av polisen. I beslutet ska anges de omständigheter som innebär att villkoren för åtgärden är uppfyllda (§ 791 d andra stycket).

I § 791 d tredje stycket regleras ändamåls- och proportionalitetsprincipen.

Det åligger leverantörer av elektroniska kommunikationsnätverk och kommunikationstjänster och administratörer av internetdomäner att bistå polisen med att genomföra blockeringsåtgärder (§ 791 d fjärde stycket). I praktiken kommer polisen att vidarebefordra domstolens beslut till leverantörer av elektroniska kommunikationsnät och kommunikationstjänster eller en eller flera administratörer av internetdomäner, som sedan kommer att ansvara för den tekniska implementeringen av en DNS-blockering. Bestämmelsen kan således tillämpas på t.ex. en internetleverantör eller en administratör i de fall där de – trots domstolens blockeringsföreläggande – inte initierar blockering av den aktuella webbplatsen (2016/1 LSF 192 s. 49).

Om den som åtgärden riktar sig mot begär det, ska polisen snarast föra ärendet till domstol. Domstolen beslutar i frågan om ingripandet får fortsätta (§ 791 d femte stycket). Av förarbetena framgår att det i praktiken är den som ansvarar för webbplatsen som kommer att kunna göra en sådan begäran. Om domstolen inte beslutar att godkänna en blockering av en webbplats, innebär det att blockeringen inte kan upprätthållas och att polisen skyndsamt måste se till att den hävs (2016/1 LSF 192 s. 50).

Polisen får i brådskande fall under vissa förutsättningar fatta interimistiskt beslut. I sådana fall ska polisen så snart som möjligt och inom 24 timmar från dagen för åtgärden hänskjuta ärendet till domstol. Om domstolen bedömer att åtgärden inte borde ha genomförts ska domstolen underrätta riksåklagaren om det eller, om beslutet har fattats av Politiets Etterrettningstjeneste (den danska motsvarigheten till Säkerhetspolisen), underrätta Justitieministeriet (§ 791 d sjätte stycket).

10.5.2 Underrättelseskyldighet

Av förarbetena framgår att polisen förväntas underrätta den person som ingreppet riktar sig mot om att domstolen har gett tillstånd till att blockera den aktuella webbplatsen. Om det inte finns kontaktuppgifter på webbplatsen och polisen inte omedelbart kan få de uppgifterna på annat sätt behöver ingen underrättelse lämnas. Det förutsätts också att om polisen får kännedom om att det inte längre finns grund för föreläggandet – t.ex. på grund av att det olagliga innehållet har tagits bort från webbplatsen – ska polisen ta bort blockeringen så snart som möjligt. Polisen är dock inte skyldig att kontinuerligt kontrollera innehållet på de blockerade webbplatserna (2016/1 LSF 192 s. 20 och 48 f.).

10.6 Regleringen i Estland

I 3 kap. § 126.1–126.13 i den estniska straffprocesslagen regleras hemliga tvångsmedel.

Enligt § 126.2 får polisen, säkerhetspolisen och tullväsendet genomföra övervakningsåtgärder bl.a. om det finns behov av att samla in information i syfte att upptäcka och förebygga eller utreda vissa i lagen särskilt angivna brott.

En sådan åtgärd som vidtas i syfte att upptäcka och förebygga brott får riktas mot personer som det finns allvarliga skäl att tro att de begår eller kommer att begå något av de i lagen angivna brotten. En åtgärd som i stället vidtas i syfte att utreda brott får riktas mot personer som är misstänkta för brott i en brottsutredning eller om det finns skäl att tro att han eller hon har begått något av de i lagen angivna brotten.

En övervakningsåtgärd får enligt § 126.3 avse att i hemlighet bl.a. observera en person, ett föremål eller ett område eller undersöka ett föremål och i hemlighet återställa det. En övervakningsåtgärd får vidare avse bl.a. att i hemlighet avlyssna eller observera information. Vid en sådan åtgärd är det tillåtet att i hemlighet bereda sig tillgång till en byggnad, ett rum, ett fordon, ett slutet område eller ett datasystem, förutsatt att det är oundgängligen nödvändigt för att uppnå operationens mål.

En åklagare eller en undersökningsdomare får, enligt § 126.4, besluta om tillstånd till övervakningsåtgärder. I brådskande fall får

åklagare besluta om tillstånd inom 24 timmar efter operationens inledande. Ett sådant tillstånd ska bl.a. innehålla uppgifter om vilken åtgärd som avses och, om det är känt, namnet på den person som åtgärden avser samt den tidsperiod som tillståndet gäller. Ett tillstånd som avser en viss person får inte överstiga ett år.

Enligt 26 § lagen om säkerhetsmyndigheterna (Security Authorities Act) får en tjänsteman vid en säkerhetsmyndighet, inom ramen för sin behörighet och för att bekämpa ett brott, på order av chefen för säkerhetsmyndigheten i hemlighet gå in i eller genomsöka bl.a. ett datasystem. Det får göras för att säkerställa den nationella säkerheten eller om det finns tillräckliga uppgifter som tyder på att ett brott håller på att förberedas eller begås och om den information som samlas in är nödvändig för att bekämpa brottet. I samband med det får uppgifter samlas in och registreras och tekniska hjälpmedel installeras och avlägsnas i det syftet samt föremål undersökas och vid behov ändras, skadas eller bytas ut.

Av 27 § framgår att ett sådant tillstånd, efter ansökan av chefen för säkerhetsmyndigheten, får beviljas av domstol utan dröjsmål och utan att förhandling hålls. Tillstånd får ges under högst två månader och kan förlängas med samma tid.

Enligt 28 § fastställs de metoder och medel som får användas av en säkerhetsmyndighet vid hemlig insamling av uppgifter i en förordning från den berörda ministern.

10.7 Regleringen i Finland

Lagen om tjänster inom elektronisk kommunikation 917/2014 syftar enligt 1 § bl.a. till att främja utbudet och användningen av elektroniska kommunikationstjänster och att säkerställa att kommunikationsnät och kommunikationstjänster på skäliga villkor är tillgängliga för alla i hela landet.

I 33 kap. regleras bl.a. hantering av informationssäkerhet och störningar. Enligt 272 §, som reglerar åtgärder för informationssäkerhet, har kommunikationsförmedlare och leverantörer av mervärdestjänster[6] och aktörer som handlar för deras räkning rätt att vidta

[6] En tjänst som baserar sig på behandling av förmedlingsuppgifter eller lokaliseringsuppgifter för andra ändamål än för att förmedla meddelanden.

nödvändiga åtgärder av teknisk natur för att sörja för informationssäkerheten. Det kan vara

a) automatisk analys av innehållet i meddelanden,

b) automatiskt förhindrande eller automatisk begränsning av förmedling och mottagande av meddelanden,

c) automatiskt avlägsnande av sådana skadliga datorprogram ur meddelandena som kan äventyra informationssäkerheten.

Åtgärderna ska vidtas i syfte att

a) upptäcka, förhindra och utreda störningar som kan inverka menligt på informationssäkerheten i kommunikationsnäten eller tjänster som anslutits till dem och informationssystemen och göra störningarna föremål för förundersökning,

b) trygga kommunikationsmöjligheterna för den som sänder eller tar emot meddelanden, eller

c) förhindra förberedelse till betalningsmedelsbedrägerier som planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.

Om det utifrån typen av meddelande, meddelandets form eller någon annan motsvarande omständighet är uppenbart att ett meddelande innehåller ett skadligt datorprogram eller ett skadligt kommando får innehållet i ett enskilt meddelande i stället behandlas manuellt. Avsändaren och mottagaren av meddelandet ska underrättas om den manuella behandlingen av innehållet, om inte underrättelsen sannolikt äventyrar att syftena med åtgärden kan uppnås.

Av 273 §, som reglerar skyldighet att avhjälpa störningar, framgår att om ett kommunikationsnät, en kommunikationstjänst eller en utrustning orsakar betydande olägenheter eller störningar i ett kommunikationsnät, en kommunikationstjänst, någon annan tjänst som anslutits till kommunikationsnätet, utrustningen, eller för kommunikationsnätets användare eller någon annan person, ska teleföretaget eller en annan innehavare av kommunikationsnätet eller utrustningen omedelbart vidta åtgärder för att avhjälpa situationen och vid behov koppla bort kommunikationsnätet, kommunikationstjänsten eller utrustningen från det allmänna kommunikationsnätet.

Åtgärderna enligt 272 och 273 §§ ska stå i proportion till den störning som avvärjs. Åtgärderna ska utföras utan att yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än vad som är nödvändigt. Åtgärderna ska avslutas om det inte längre finns förutsättningar för att vidta dem.

Transport- och kommunikationsverkets föreskrifter, Traficom/248815/03.04.05.00/2022 M67 kompletterar bestämmelserna i 272 § lagen om tjänster inom elektronisk kommunikation. Föreskrifterna trädde i kraft den 1 september 2024. De innehåller bl.a. bestämmelser om skyldigheter för teleföretag att filtrera skadlig trafik i internetaccesstjänster (4 kap. 22 §) och filtrering av text- och multimediemeddelandetrafik (5 kap. 24 §) och e-posttrafik (5 kap. 26 §). Vidare finns bestämmelser om skyldighet för teleföretag att koppla bort ett kundabonnemang från det allmänna kommunikationsnätet om kommunikationstjänstens informationssäkerhet väsentligen äventyras av orsaker som beror på utgående eller inkommande trafik och om det inte är möjligt att sörja för kommunikationstjänstens informationssäkerhet genom att filtrera skadlig trafik (4 kap. 23 §).

I rekommendationen Traficom/511921/03.04.05.01/2020 specificeras olika tekniska filteringsåtgärder, som blockering eller begränsning av trafik vid t.ex. ett överbelastningsangrepp. Av rekommendationen framgår bl.a. följande. Ett teleföretag kan temporärt blockera eller begränsa trafiken till en viss kommunikationsport till den delen och så länge det är nödvändigt för att upprätthålla datasäkerheten. När en sådan blockering görs är det viktigt att

a) anpassa skyddsåtgärderna för att matcha allvaret i det hot som ska hanteras,

b) se till att åtgärderna inte begränsar yttrandefriheten, meddelandesekretessen eller integritetsskyddet mer än vad som är nödvändigt, och

c) åtgärderna avbryts om det inte längre finns förutsättningar för dem.

När filtrering övervägs är det alltid viktigt att bedöma om filtrering överhuvudtaget är nödvändig, och i så fall hur länge den är nödvändig. Filtreringsåtgärder som vidtas av datasäkerhetsskäl bör i regel vara tillfälliga och avbrytas när hotet har undanröjts. Varje teleföre-

tag avgör på grundval av sina egna observationer av hot mot informationssäkerheten om filtrering är nödvändig och hur länge den ska pågå för att upprätthålla informationssäkerheten i nätet, i de tjänster som tillhandahålls via nätet eller i slutanvändarnas terminaler.

10.8 Regleringen i Frankrike

Lagen om inre säkerhet (”Code de la sécurité intérieure”, CSI) från år 2012 infördes för att samla alla lagar och förordningar som rör Frankrikes inre säkerhet.

Av avdelning VIII i CSI, som reglerar underrättelseverksamhet, framgår att de specialiserade underrättelsetjänsterna enbart i syfte att utföra sina respektive uppdrag får använda de tekniker som nämns i avdelning V. Det får göras för att samla in underrättelser som rör försvaret och främjandet av följande grundläggande intressen för nationen

1. nationell självständighet, territoriell integritet och nationellt försvar,
2. viktiga utrikespolitiska intressen, Frankrikes europeiska och internationella åtaganden och förebyggande av alla former av utländsk inblandning,
3. Frankrikes viktigaste ekonomiska, industriella och vetenskapliga intressen,
4. förebyggande av terrorism,
5. förebyggande av

a) angrepp mot republikens institutionella struktur,

b) åtgärder som syftar till att upprätthålla eller återupprätta grupper som upplösts enligt en viss angiven bestämmelse,

c) kollektivt våld som sannolikt allvarligt stör den allmänna ordningen,

d) organiserad brottslighet, och

e) spridning av massförstörelsevapen.

Bestämmelserna i fråga omfattar inte bl.a. åtgärder som vidtas enbart i syfte att säkerställa övervakning och kontroll av radiosändningar.

Av artikel L853-2 framgår att om information inte kan samlas in på något annat lagligt sätt, får särskilt utsedda tjänstemän använda tekniska anordningar för att få tillgång till, registrera, lagra och överföra uppgifter som lagras i ett datasystem. Vidare får de använda tekniska anordningar för att få tillgång till, registrera, lagra och överföra sådana uppgifter i ett datasystem som visas på en skärm för användaren av ett datasystem, medan de matas in, eller medan de tas emot och överförs.

Tillträde till ett fordon, en privat lokal eller en bostad får tillåtas endast under vissa förutsättningar.

Ett tillstånd till sådana åtgärder får ges under högst två månader.

Den nationella kommissionen för kontroll av underrättelsetekniker, som ska underrättas om verkställighet av åtgärderna, ska granska deras proportionalitet och laglighet. Kommissionen kan när som helst utfärda en rekommendation om att åtgärden ska avbrytas och att insamlade uppgifter ska förstöras.

Premiärministern beslutar, efter samråd med den nationella kommissionen för kontroll av underrättelsetekniker, om tillstånd till åtgärder. När tillstånd utfärdas efter ett avstyrkande från den nationella kommissionen för kontroll av underrättelsetekniker, ska ärendet omedelbart hänskjutas till statsrådet av kommissionens ordförande eller av en av kommissionens ledamöter. Premiärministerns beslut får endast verkställas omedelbart om han eller hon har beordrat det.

En begäran om tillstånd ska innehålla bl.a. uppgifter om

a) den eller de tekniker som ska användas,

b) det eller de syften som ska uppnås med åtgärden,

c) skälen för åtgärden,

d) den tidsperiod som åtgärden får verkställas, och

e) den eller de personer, platser eller fordon som åtgärden rör (en person vars identitet är okänd får betecknas utifrån bl.a. sin position, plats eller fordon).

10.9 Regleringen i Nederländerna

10.9.1 Åtgärder i brottsutredande syfte

Databrottslagen (Wet computercriminaliteit III, 2019) trädde i kraft den 1 mars 2019 och innebar ändringar i både strafflagen och straffprocesslagen.

Enligt straffprocesslagen får undersökningsdomare, åklagare och särskilt utsedda utredare genomföra husrannsakan på en plats för att registrera uppgifter som lagras eller registreras på ett datamedium på den platsen, om det finns misstanke om att ett i lagen särskilt angivet brott eller brott som kan leda till fängelse i fyra år eller mer har begåtts eller upptäcks på bar gärning.

Åklagare får, efter att ha beslagtagit ett datasystem och fått tillstånd från undersökningsdomaren, ålägga en utredande tjänsteman att under en period av tre dagar efter beslaget granska eller registrera uppgifter som lagrats i systemet. Efter tillstånd från undersökningsdomare får granskningen pågå under en period om högst tre månader efter beslaget. Åklagaren får förlänga ett sådant beslut med en period av högst tre månader, totalt med högst sex månader.

I beslutet ska det bl.a. anges

a) brottet och, om känt, namnet eller annars en så exakt beskrivning som möjligt av den misstänkte,

b) de omständigheter som visar att förutsättningarna för tillstånd är uppfyllda,

c) namnet eller, om inte det är känt, den mest exakta möjliga beteckningen på användaren av det beslagtagna datasystemet,

d) typen av datasystem,

e) det sätt som beslutet ska verkställas på, och

f) den period som tillståndet ska gälla.

I brådskande fall får åklagare meddela ett muntligt beslut. I sådant fall ska åklagaren meddela ett skriftligt beslut inom tre dagar. Åklagarens beslut upphör om beslaget av ett datasystem upphävs.

Om ett beslagtaget datasystem är biometriskt säkrat eller om informationen är biometriskt krypterad i form av ett fingeravtryck, en iris eller en ansiktsbild, får åklagare beordra en utredningsman att

upphäva säkerheten eller krypteringen. För att verkställa det, får utredningsmannen vidta de åtgärder som rimligen är nödvändiga.

I den utsträckning utredningen särskilt kräver det, får ett föreläggande meddelas den som skäligen kan misstänkas ha kunskap om säkerhetsmetoden för ett datasystem, att ge tillgång till det eller delar av det genom att göra kunskapen tillgänglig. Detsamma gäller den som skäligen kan misstänkas ha kännedom om krypteringsmetoden om det finns krypterade uppgifter i ett datasystem. Ett sådant föreläggande får dock inte meddelas den misstänkte.

Det krävs samtycke för undersökning av datasystem där uppgifter har matats in av eller på uppdrag av journalister eller vittnen som anförtrotts uppgifter på grund av sin rang, sitt yrke eller sitt ämbete.

Om en undersökning av ett datasystem leder till en registrering av data eller att data blir oåtkomlig, ska den eller de berörda personerna underrättas om det så snart som möjligt, dock inte om det rimligen inte är möjligt.

Så snart det visar sig att de uppgifter som registrerats under en husrannsakan saknar relevans för utredningen ska de förstöras. Åklagare får besluta att uppgifter som registrerats vid husrannsakan får användas i en annan brottsutredning än den för vilken åtgärden genomfördes.

Åklagare eller undersökningsdomare får, om det vid en undersökning av ett datasystem kommer fram uppgifter om vilka eller med hjälp av vilka ett brott har begåtts, besluta att göra uppgifterna oåtkomliga i den utsträckning som är nödvändig för att få brottet att upphöra eller för att förhindra att nya brott begås. Att göra data oåtkomliga innebär att åtgärder vidas för att förhindra att tredje part får kännedom om eller använder uppgifterna eller sprider uppgifterna, vilket delvis innebär att uppgifterna tas bort från datasystemet, samtidigt som uppgifterna behålls för att kunna användas i det straffrättsliga förfarandet.

Vid misstanke om ett i lagen särskilt angivet brott eller brott som kan leda till fängelse i fyra år eller mer, får åklagare förelägga en leverantör av en kommunikationstjänst att omedelbart vidta alla åtgärder som rimligen kan krävas av leverantören för att göra vissa lagrade eller överförda uppgifter oåtkomliga, i den mån det är nödvändigt för att få ett brott att upphöra eller för att förhindra att nya brott begås.

Undersökningsdomare får efter ansökan av åklagare besluta om ett sådant tillstånd, som ska ange

a) brottet,

b) de omständigheter av vilka det framgår att det är nödvändigt att göra uppgifterna oåtkomliga för att brottet ska upphöra eller för att förhindra nya brott, och

c) vilka uppgifter som ska göras oåtkomliga.

Vid misstanke om ett i lagen särskilt angivet brott eller brott som kan leda till fängelse i fyra år eller mer och som på grund av sin art eller sitt samband med andra brott som den misstänkte har begått utgör ett allvarligt brott mot rättsordningen, får åklagaren, om utredningen brådskar, ålägga en särskilt utsedd utredare att bereda sig tillgång till ett datasystem som används av den misstänkte och, med eller utan tekniskt hjälpmedel, undersöka systemet. Det får göras bl.a. i syfte att

a) fastställa vissa egenskaper hos datasystemet eller användaren, som identitet eller plats, och registrera dem,

b) verkställa ett tillstånd om att registrera hemlig kommunikation med hjälp av ett tekniskt hjälpmedel eller avlyssna hemlig kommunikation som tillhandahålls av en leverantör av kommunikationstjänster, och

c) i fråga om bl.a. ett brott som kan bestraffas med fängelse i åtta år eller mer, registrera uppgifter som lagras i datasystemet, eller som lagrats först efter att tillståndet beslutats, i den utsträckning som rimligen är nödvändig för att utreda brottet.

Undersökningsdomare beslutar om ett sådant tillstånd efter ansökan av åklagare. I beslutet ska bl.a. anges

a) brottet och, om det är känt, namnet eller annars en så exakt beskrivning som möjligt av den misstänkte,

b) ett nummer eller annan indikation som kan användas för att identifiera datasystemet och, om det är känt, om uppgifterna inte lagras i Nederländerna,

c) de omständigheter av vilka det framgår att förutsättningarna för tillståndet är uppfyllda,

d) arten och funktionen hos det tekniska hjälpmedlet som används för att verkställa tillståndet, och

e) de åtgärder som ska utföras.

Tillstånd får ges för högst fyra veckor och kan förlängas med samma tid. Beslutet får ändras, kompletteras, förlängas eller upphävas. Om det finns brådskande skäl får ett sådant beslut meddelas muntligen. I sådant fall ska åklagaren meddela ett skriftligt beslut inom tre dagar. Det finns vidare bestämmelser om bl.a. krav på att det tekniska hjälpmedlet tas bort och om tillsyn över tillstånden. Motsvarande gäller vid indikationer på att ett terroristbrott har begåtts.

Liknande bestämmelser finns om brottet på grund av sin art eller sitt samband med andra brott planerats eller utförts i ett organiserat sammanhang och datasystemet används av en person som det finns skälig misstanke om att han eller hon är inblandad i planeringen eller utförandet av ett sådant brott. Beslutet om tillstånd ska i sådant fall även innehålla en beskrivning av den organiserade gruppen och, om det är känt, namnet eller annars en så exakt beskrivning som möjligt av den person som misstänks vara inblandad i planeringen eller utförandet av brottet.

Bestämmelserna kompletteras av ett beslut om genomsökning av datasystem från år 2024. Det reglerar hur åtgärderna närmare får verkställas, bl.a. när det gäller utformningen av de tekniska hjälpmedel som får användas.

Domstol får besluta att uppgifter, som har gjorts oåtkomliga i samband med ett brott eller med hjälp av vilka ett brott har begåtts ska förstöras, i den mån förstörandet är nödvändigt för att förhindra att nya brott begås. Om så inte sker ska uppgifterna i stället göras tillgängliga på nytt för administratören av datasystemet.

Berörda parter kan skriftligen klaga på de olika beslut om tillstånd avseende datasystem som har redovisats. Domstolen ska pröva klagomålet så snart som möjligt.

10.9.2 Åtgärder i underrättelseverksamhet

I lagen om underrättelse- och säkerhetstjänster från år 2017 regleras den civila underrättelse- och säkerhetstjänstens (AIVD) och den militära underrättelse- och säkerhetstjänstens (MIVD) verksamhet. De har bl.a. i uppdrag att genomföra utredningar som rör allvarliga misstankar om att individer och organisationer utgör ett hot mot statens säkerhet eller andra viktiga intressen, genomföra utredningar som rör andra länder, vidta främjande åtgärder för att skydda viktiga statliga intressen och utarbeta hot- och riskanalyser i olika avseenden.

En tillfällig lag för AIVD och MIVD att utreda länder med ett offensivt cyberprogram, massdata och andra specifika anläggningar trädde i kraft i januari 2024 och upphör att gälla fyra år därefter. Den kompletterar lagen om underrättelse- och säkerhetstjänster när det gäller det uppdrag som tjänsterna har. Den tillfälliga lagen ger tjänsterna i uppdrag att utföra utredningar av länder med ett s.k. offensivt cyberprogram mot Nederländerna eller nederländska intressen.

Lagen om underrättelse- och säkerhetstjänster tillåter övervakning och registrering av data om fysiska personer eller egendom med eller utan teknisk utrustning.

Enligt lagen om underrättelse- och säkerhetstjänster får tjänsterna

a) undersöka de tekniska egenskaperna hos datasystem som är anslutna till ett kommunikationsnätverk, och

b) bereda sig tillgång till ett datasystem, oavsett om det görs med hjälp av ett tekniskt hjälpmedel, falska signaler, falska nycklar, falsk identitet. Det gäller även en tredje parts system (förutom punkten c). I det sammanhanget får tjänsterna även

c) bryta mot säkerhetsåtgärder,

d) genomföra tekniska åtgärder för att upphäva kryptering av data som lagras eller behandlas i datasystemet,

e) genomföra tekniska åtgärder som möjliggör övervakning, registrering, avlyssning och inspelning av data, och

f) hämta data som lagras eller behandlas i datasystemet.

Relevant minister beslutar om tillstånd till en sådan åtgärd. Enligt den tillfälliga lagen får dock även chefen för den relevanta tjänsten

besluta om ett sådant tillstånd, vilket tillsynsmyndigheten ska underrättas om.

En begäran om tillstånd ska bl.a. ange

a) identiteten på den person eller organisation som åtgärden avser,

b) en beskrivning av den utredning som är kopplad till åtgärden,

c) en beskrivning av det syfte som ska uppnås med åtgärden,

d) skälet till att åtgärden anses nödvändig och proportionerlig,

e) en beskrivning av de tekniska risker som är förknippade med åtgärden, och

f) ett nummer, en teknisk egenskap eller annan beteckning genom vilken datasystemet kan identifieras.

Tillståndet omfattar även, enligt den tillfälliga lagen, en rätt att få tillgång till ett annat datasystem som används av personen eller organisationen i fråga, i den mån det ersätter eller kompletterar det datasystem för vilket tillståndet ursprungligen beviljades.

Tjänsterna har rätt, efter att relevant minister beslutat om tillstånd, att kontakta den person som rimligen misstänks ha kunskap om eventuell krypteringsmetod för uppgifter som lagras eller behandlas i datasystemet och begära att han eller hon samarbetar för att dekryptera uppgifterna antingen genom att lämna ut den informationen eller genom att upphäva krypteringen.

Enligt lagen om underrättelse- och säkerhetstjänster får relevant minister besluta om tillstånd för tjänsterna, efter ansökan från chefen för den relevanta tjänsten, att avlyssna, ta emot och spela in alla former av samtal, telekommunikation eller dataöverföring genom ett datasystem med hjälp av ett tekniskt hjälpmedel, oavsett var det sker. Den rätten omfattar även att upphäva kryptering av samtal, telekommunikation eller dataöverföring.

En begäran om tillstånd ska, utöver de uppgifter som nyss nämnts, ange

a) ett nummer eller en teknisk egenskap, och

b) information om identiteten på den person eller organisation som åtgärden avser.

Ett tillstånd som avser att ta emot eller spela in telekommunikationer omfattar även andra nummer eller tekniska egenskaper knutna till den berörda personen eller organisationen som blir kända efter det att tillståndet beviljats.

Tjänsterna får enligt lagen om underrättelse- och säkerhetstjänster bl.a. undersöka uppgifter som inhämtats genom den åtgärd som senast nämnts, i syfte att

a) fastställa telekommunikationernas egenskaper och art, och

b) fastställa identiteten på den person eller organisation som är knuten till telekommunikationerna.

Efter tillstånd av relevant minister har tjänsterna rätt att vidta åtgärder mot den som skäligen kan misstänkas ha kunskap om krypteringsmetoden för samtalen i fråga, telekommunikations- och överföring av uppgifter för att han eller hon ska göra kunskapen om hur data dekrypteras tillgänglig eller upphäva krypteringen.

Underrättelse- och säkerhetstjänsterna ska ha tillträde till vilken plats som helst, i den utsträckning det rimligen är nödvändigt bl.a. för att

a) installera, byta ut eller ta bort observations- och registreringsanordningar och utföra därmed sammanhängande förberedande verksamhet,

b) installera, byta ut eller ta bort spårningsanordningar, positioneringsutrustning och registreringsanordningar och utföra därmed sammanhängande förberedande verksamhet, och

c) genomföra vissa specifika åtgärder, inklusive installation, utbyte eller borttagning av en teknisk anordning, och utföra därmed sammanhängande förberedande verksamhet.

10.10 Regleringen i Storbritannien

I del 5 i Investigatory Powers Act (IPA) regleras påverkan på utrustning. Ett beslut om sådan påverkan kan avse ett tillstånd till riktad påverkan på utrustning eller ett tillstånd till riktad undersökning.

Enligt 99 § får sådan påverkan verkställas med hjälp av någon utrustning i syfte att få del av kommunikation (som definieras i 135 §),

utrustningsuppgifter (som definieras i 100 §) och annan information. Det får göras genom

1. övervakning, observation eller avlyssning av en persons kommunikation eller andra aktiviteter, eller
2. inspelning av allt som övervakas, observeras eller avlyssnas.

Riktad påverkan på utrustning får även användas på andra sätt om det är nödvändigt för att uppnå det angivna syftet med tillståndet.

Ett beslut om riktad påverkan får enligt 101 § avse en eller flera av följande utrustningar

a) utrustning som tillhör, används av eller innehas av en viss person eller organisation,
b) utrustning som tillhör, används av eller innehas av en grupp personer som har ett gemensamt syfte eller som utövar eller kan utöva en viss verksamhet,
c) utrustning som tillhör, används av eller innehas av mer än en person eller organisation, om störningen görs i syfte att genomföra en specifik utredning eller operation,
d) utrustning på en viss plats,
e) utrustning på mer än en plats om påverkan görs i syfte att genomföra en specifik utredning eller operation,
f) utrustning som används eller kan komma att användas för en viss verksamhet eller verksamheter av en viss typ,
g) utrustning som används eller kan komma att användas för att testa, underhålla eller utveckla förmåga att påverka utrustning i syfte att få tillgång till kommunikation, utrustningsuppgifter eller annan information, och
h) utrustning som används eller kan komma att användas för utbildning av personer som utför eller sannolikt kommer att utföra sådana ingrepp på utrustning.

En hög politisk regeringsföreträdare[7] får, efter ansökan av någon av cheferna för säkerhets- och underrättelsetjänsterna eller chefen för

[7] Minister eller statssekreterare.

den militära underrättelsetjänsten, besluta om tillstånd till riktad påverkan av utrustning, om åtgärden är proportionerlig för att uppnå ändamålet med åtgärden och om vissa närmare angivna rättssäkerhetsgarantier är uppfyllda. Vidare får tillstånd beslutas om åtgärden är nödvändig för den nationella säkerheten, i syfte att förebygga eller upptäcka allvarlig brottslighet eller i intresset av ekonomisk välfärd, i den mån de intressena också är relevanta för den nationella säkerheten och intressena avser att få uppgift om handlingar vidtagna av eller avsikter hos personer utanför de brittiska öarna (102, 104 och 105 §§).

Det krävs också att tillståndet har godkänts av en ”Judicial Commissioner”, utom i brådskande fall, (102 §).

Under liknande förutsättningar får vissa chefer för brottsbekämpande myndigheter, på ansökan av en lämplig underlydande person, besluta om tillstånd till riktad påverkan på utrustning om åtgärden har viss koppling till brittiska öarna (106 och 107 §§).

Även skotska regeringstjänstemän får under vissa förutsättningar besluta om tillstånd (103 §).

I 111–114 §§ regleras vissa rättssäkerhetsgarantier som ska beaktas vid besluten.

Enligt 115 § ska i tillståndet anges om åtgärden avser utrustning som tillhör, används av eller innehas av en viss person eller organisation, namnet på eller en beskrivning av den person eller organisation som åtgärden riktar sig mot. I tillstånd som riktar sig mot en grupp som har ett gemensamt syfte eller som bedriver (eller kan bedriva) viss verksamhet ska syftet eller verksamheten anges och namnet på eller en beskrivning av så många av de personerna som det rimligen är praktiskt möjligt att namnge eller beskriva anges. Om åtgärden avser utrustning på en viss plats, ska platsen beskrivas och den operation eller utredning som avses om åtgärden avser flera platser. Om åtgärden avser utrustning som används eller kan komma att användas för viss verksamhet eller verksamheter av särskild karaktär, ska verksamheten eller verksamheterna beskrivas.

Åtgärden får pågå i högst sex månader (116 §) och tillståndet får förlängas om åtgärden är nödvändig och proportionerlig (117 §).

Den som beslutat om tillstånd får när som helst ändra beslutet bl.a. genom att lägga till, ändra eller ta bort namnet eller beskrivningen av en person, organisation eller utrustning som tillståndet avser. I brådskande fall får den som ska verkställa beslutet, eller en chef för

den personen, ändra tillståndet (118–120 §§). I 121 och 122 §§ regleras underrättelse om och godkännande av ett ändrat tillstånd. I 123 och 124 §§ anges under vilka förutsättningar som ett tillstånd enligt 106 § får ändras och godkännande av sådana brådskande beslut.

I 125 § regleras under vilka förutsättningar som åtgärden ska avbrytas.

I 129 och 130 §§ behandlas särskilda rättssäkerhetsgarantier som ska beaktas vid lagring och utlämnande av uppgifter som hämtats in enligt tillstånden, såväl nationellt som internationellt.

I del 9 regleras bl.a. definitioner av telekommunikation (261 §) och vissa andra kommunikationer (262 §) samt allmänna definitioner (263 och 264 §§).

Påverkan på utrustning kan utföras antingen på distans, i närheten av utrustningen eller genom fysisk interaktion med utrustningen. Åtgärderna varierar i komplexitet. De kan verkställas antingen genom att data laddas ner från en mobil enhet när den lämnas obevakad, att någons inloggningsuppgifter används för att få tillgång till data som finns på en dator eller att befintliga sårbarheter i en programvara utnyttjas för att få kontroll över enheter eller nätverk för att fjärrextrahera material eller för att övervaka användaren av enheten (Equipment Interference Code of Practice, Home Office, June 2025, s. 15).

10.11 Regleringen i Tyskland

Enligt § 100 b straffprocesslagen får tekniska medel användas för att få hemlig tillgång till ett informationssystem som används av en viss person och för att extrahera data från det systemet om

a) någon i egenskap av gärningsman eller medgärningsman misstänks för att ha begått något av de brott som räknas upp i paragrafen, antingen i fullbordad form eller i form av försök till sådant brott,

b) brottet är grovt, och

c) andra åtgärder för att fastställa omständigheterna eller den misstänktes vistelseort skulle vara väsentligt svårare eller inte erbjuda några utsikter till framgång.

Åtgärden får endast riktas mot en person som är misstänkt för brottet. En sådan åtgärd mot andra personers informationssystem är dock tillåten om det kan antas att

a) den misstänkte använder någon annans informationssystem, och

b) ingreppet i den misstänktes informationssystem inte kommer att leda till fastställande av omständigheter eller till fastställande av var en medmisstänkt person befinner sig.

Åtgärden får vidtas även om den oundvikligen drabbar andra personer.

Av förarbetena framgår att åtgärden utförs med hjälp av en skadlig kod, en statlig eller federal s.k. trojan och innebär, till skillnad från hemlig telekommunikationsövervakning, att inte endast nyligen tillagt kommunikationsinnehåll kan övervakas, utan såväl informationssystemets användning som allt innehåll som lagras på det, inklusive t.ex. inbyggda kameror.[8]

Enligt § 100 e andra stycket straffprocesslagen får domstol efter ansökan av åklagare besluta om tillstånd till hemlig distansundersökning av informationssystem. Tillstånd får inte beviljas för mer än en månad och får förlängas med längst en månad åt gången. I beslutet ska det bl.a. anges vem som åtgärden riktar sig mot om det är känt och det misstänkta brottet, vilken åtgärd tillståndet avser, omfattningen och varaktigheten av tillståndet och när åtgärden ska upphöra. De väsentliga övervägandena om åtgärdens nödvändighet och proportionalitet ska också anges i beslutet.

Av fjärde stycket framgår att åtgärderna ska upphöra om de omständigheter som legat till grund för åtgärden inte längre är uppfyllda.

[8] (Plenarprotokoll, Bundesrat – 959, Sitzung – 7, Juli 2017, s. 355 och Deutscher Bundestag, Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz, Drucksache 18/12785, 20 Juni 2017, s. 53 f.).

11 Myndigheternas beskrivning av behovet

11.1 Polismyndigheten

Kriminella utnyttjar i allt större omfattning teknologi för att utsätta personer för brott. En utmaning när det gäller cyberbrott är enligt Polismyndigheten att både digitala spår och infrastruktur är flyktiga och att sårbarheter snabbt kan täppas igen. Virtuell datalagring och angripande servrar kan byta plats inom sekunder tack vare molnteknologi och botnet. Information kan därmed snabbt försvinna eller i vart fall hamna utom räckhåll för nationella rättssystem. För att brottsbekämpande myndigheter ska ha en effektiv ingripandeförmåga krävs att myndigheterna har förutsättningar att agera snabbt, ibland direkt, innan de traditionella rättsliga samarbetsvägarna hinner aktiveras.

Ett särskilt problem är det förhållandevis nya fenomenet crime as a service. Genom att ”annonsera” brottsliga uppdrag på digitala plattformar lockar kriminella nätverk in framför allt ungdomar i mycket allvarlig kriminalitet. Det rör sig ofta om tidigare ostraffade personer som åtar sig uppdrag för ekonomisk vinning eller som pressas att begå brott.

Polismyndigheten har samma möjligheter att utreda och dokumentera både renodlade cyberbrott och cyberrelaterade brott som andra traditionella brott i den fysiska världen, även om internationella aspekter kan göra utredningarna mer tidsödande och komplicerade. Myndighetens brottsbekämpande uppdrag omfattar både fysisk och digital miljö. Dagens polisiära befogenheter är emellertid i princip begränsade till den fysiska miljön. Det har lett till att polisiära metoder och verktyg för att ingripa i den fysiska miljön i varierande grad har kommit att förlora sin verkan. Polisens möjligheter

att förhindra, störa och avbryta brott i digital miljö är mycket begränsade, eftersom sådana åtgärder som utgångspunkt innebär dataintrång enligt 4 kap. 9 c § brottsbalken. Konsekvensen av att polisen inte har tillräckligt rättsligt stöd för att ingripa är att kriminella kan agera alltför fritt i den miljön. Kvalificerade cyberbrott som ransomware, informationsstölder och överbelastningsangrepp vållar samhället mycket stora kostnader och enskilda angrepp kan vara både samhälls- och systemhotande. Enligt Polismyndigheten är Sverige ett av de länder i världen som har störst problem med illegala marknadsplatser på Darknet. Genom dem säljs bl.a. vapen, narkotika, brottsupplägg och övergreppsmaterial. Det är viktigt att polisen får möjlighet att ingripa mot sådana brott för att Sverige inte ska vara ett attraktivt land för att begå cyberbrott och cyberrelaterade brott i eller från och för att polisen ska kunna upprätthålla allmän ordning och säkerhet.

Polismyndigheten behöver få rätt att ingripa i digitala system för att förhindra och avbryta brottslig verksamhet eller pågående brott innan de fullbordas för att myndigheten ska kunna fullgöra sitt uppdrag. Att avbryta brott kan i ett enskilt fall ha ett högre värde för Polismyndigheten och för samhället i stort än att lagföra de som ligger bakom brotten.

Polismyndigheten har identifierat ett antal förmågor som enligt myndigheten behövs för att effektivt kunna ingripa mot cyberbrott och cyberrelaterade brott. De är

- att kartlägga digitala kommunikationsflöden i syfte att överblicka kriminell digital infrastruktur,
- att påverka tillgängligheten till digitala plattformar, tjänster eller system, och
- att radera, ändra eller lägga till information på digitala plattformar, tjänster eller system.

För att kunna avbryta pågående cyberbrott och cyberrelaterade brott behöver polisen få rätt att kringgå eller bryta systemskydd för att på så sätt kunna kartlägga och, i förlängningen, kunna ingripa mot den brottsliga verksamheten eller brotten genom att exempelvis

- blockera digital kommunikation genom att med aktiva åtgärder, t.ex. ett överbelastningsangrepp, begränsa tillgängligheten till digital kommunikation eller it-infrastruktur,
- överta en server som leder ett angrepp eller en plattform för kriminell aktivitet genom att utestänga systemägaren från teknisk tillgång till systemet, och
- kryptera en server eller radera innehåll av övergreppsmaterial så att brottslig verksamhet inte kan fortgå.

Polismyndigheten behöver också kunna få tillträde till platser som är skyddade mot intrång, i syfte att installera teknisk utrustning som behövs för ingripanden i digital miljö.

Polismyndigheten understryker att en ny reglering inte bör bygga på en uppräkning av brott vid vilka åtgärderna får användas utan vara generell. En effektiv förmåga att ingripa kommer att kräva sekundoperativa eller åtminstone minutoperativa beslut. Tillgång till kriminella tjänster eller plattformar kan snabbt upphöra, eftersom även kriminella och hotaktörer har sina egna säkerhets- och varningssystem. Utgångspunkten bör därför vara att Polismyndigheten bör få fatta beslut om åtgärder för att kunna agera tillräckligt snabbt. Det bör ske på chefsnivå alternativt av några få personer inom en specialistgrupp.

Fler länder, t.ex. Australien, Belgien, Estland, Frankrike, Nederländerna, Storbritannien, Tyskland och USA har enligt Polismyndigheten infört mer offensiva lagar som ger deras brottsbekämpande myndigheter möjligheter att ingripa utanför sina egna gränser i syfte att störa, avbryta eller förstöra illegala digitala aktiviteter.

11.2 Säkerhetspolisen

Eftersom internet har en global räckvidd kan skyddsvärd information från hela världen vara åtkomlig och hämtas in av främmande makt genom att utnyttja svagheter i cybersäkerheten. Främmande makt kan förbereda sin inhämtning genom att skaffa tillgång till ett stort antal internetanslutna enheter i olika länder, t.ex. genom att göra intrång i privatpersoners wifiroutrar eller genom att hyra virtuella servrar av olika datacenter. En kedja av sådana enheter (ett ano-

nymiseringsnätverk) används sedan för själva inhämtningen, vilket gör det svårt att spåra den som faktiskt skaffar sig informationen. Internet har gjort det lättare för främmande makt att kunna undgå kartläggning och att hämta in skyddsvärd information på ett relativt enkelt och riskfritt sätt, när som helst under dygnet. När främmande makt bedriver underrättelseinhämtning utnyttjas medvetet olika begränsningar som gäller i andra länders lagstiftning för att försvåra för de myndigheter som har till uppgift att upptäcka och stoppa sådan inhämtning. Det gäller även den svenska lagstiftningen.

I och med att internet och dess infrastruktur är gränsöverskridande uppstår det jurisdiktionsfrågor vid cyberbrott och cyberrelaterade brott. Myndigheter i vissa andra länder har större möjligheter att agera än de svenska. Säkerhetspolisen anser att en lösning på jurisdiktionsfrågan kan vara att regleringen bygger på att det finns eller har funnits en inblandad dator i Sverige.

Många gånger finns det inte någon fysisk person som utför ett cyberangrepp, exempelvis olovlig nedladdning av information från en persons e-postkonto, eftersom en sådan åtgärd kan utföras genom automatiserade processer. Säkerhetspolisen har i dag inte några rättsliga möjligheter att använda hemliga tvångsmedel i sådana fall, eftersom lagstiftningen förutsätter att det finns en misstänkt person. Hemlig avlyssning av privat utrustning, som utan att ägaren vet om det används av främmande makt, är ett annat problem, eftersom den person som äger utrustningen inte kan misstänkas för något brott.

För att kunna fullgöra sitt uppdrag att förhindra bl.a. spioneri och terrorism, som begås med hjälp av digital infrastruktur, behöver Säkerhetspolisen samma rättsliga verktyg som i den fysiska världen.

Säkerhetspolisen efterfrågar, när det t.ex. gäller en nätverksansluten enhet, rättsliga möjligheter att kunna göra följande

- lyssna på trafik till och från en enhet i syfte att kartlägga ett angrepp, t.ex. för att ta reda på vem eller vad det riktas mot,
- läsa av information från enheten, t.ex. för att komma åt och analysera den skadliga koden,
- förändra information på enheten för att kunna förhindra framtida utnyttjande genom att antingen
  - ta bort programvara eller
  - lägga till den senaste säkerhetsuppdateringen, och

- påverka enhetens tillgänglighet, exempelvis genom att förhindra att meddelanden kommer fram.

Åtgärder av det nu angivna slaget bör inte påverka den personliga integriteten på samma sätt som när det handlar om någon persons datatrafik. Den trafik som Säkerhetspolisen behöver kunna inhämta uppgifter om har inte genererats av den person som äger den angripna utrustningen, utan trafiken i fråga passerar endast via utrustningen på sin väg mellan angriparen och hans eller hennes mål. Sådana enheter är brottsverktyg enligt svensk rätt, men inte enligt utländsk rätt. I synnerhet om en privatperson inte sparar annan information på enheten, bör det enligt Säkerhetspolisen inte vara integritetskränkande att vidta sådana åtgärder som nyss nämnts. Det bör enligt Säkerhetspolisens mening ses som ett större bekymmer att främmande makt använder en persons wifirouter som verktyg för att t.ex. spionera på Sverige, än att en svensk myndighet riktar åtgärder mot samma utrustning för att förhindra allvarliga brott.

Att förhindra, störa och avbryta cyberrelaterade brott bör enligt Säkerhetspolisen regleras i en ny lag i stället för i någon av de befintliga lagarna. Eftersom det rör sig om minutoperativa åtgärder riskerar de att bli verkningslösa om åklagare eller domstol ska fatta beslut. Säkerhetspolisen behöver kunna agera snabbt. Säkerhetspolisen bör därför få fatta beslut om aktuella preventiva åtgärder. Möjligen kan åtgärderna underställas domstol eller Säkerhets- och integritetsskyddsnämnden i ett senare skede för efterhandskontroll.

Det finns lagstiftning som möjliggör effektiva preventiva åtgärder mot cyberbrott och cyberrelaterade brott i andra länder, t.ex. England, Norge, Finland och Estland.

11.3 Tullverket

Tullverket delar uppfattningen att den ökade digitaliseringen och den nya tekniken ger kriminella nya möjligheter att begå brott. Narkotika, vapen, explosiva varor och andra varor smugglas in i landet i både stora och små mängder. Den småskaliga införseln kan ha hög frekvens och sammantaget resultera i att bl.a. stora mängder narkotika förs in i landet. Tullverket ser en ökning av beslag i post- och kurirflödet och det finns uppgifter som anger att sådan smuggling

till stor del har sin grund i försäljning på marknadsplatser online. Det är i många fall svårt att få fram vilka servrar som används för marknadsplatserna och vem eller vilka som ligger bakom dem. Samtidigt orsakar de en omfattande samhällsskada. Det är även vanligt att grov smuggling har digitala inslag och att planering och genomförande sköts med stöd av digital teknik.

Det skulle vara effektivt att bl.a. kunna stänga ned eller ta över marknadsplatser för illegala varor. Genom en sådan åtgärd skulle flödet av illegala varor in till Sverige påverkas och smuggling skulle både kunna förebyggas och förhindras. Förmågan att utreda smugglingsbrott skulle också öka. De andra åtgärder som polisen tar upp i sin behovsbeskrivning är viktiga även för Tullverket. Tullverket ser alltså behov av att, på samma sätt som polisen, få möjlighet att ingripa mot cyberrelaterade brott och en möjlighet att avbryta sådan brottslighet i digital miljö. Det är därför viktigt att regleringen utformas så att den även ger Tullverket möjlighet att använda befogenheterna.

Tullverket ser särskilt behov av ingripanden vid brottslighet som gäller smuggling av vapen, narkotika och explosiva varor, men delar Polismyndighetens uppfattning att en ny reglering inte bör knytas till en uppräkning av brott. Tullverket menar att utökade befogenheter i digital miljö skulle innebära en ökad förmåga för Tullverket att ingripa mot högt uppsatta personer inom de kriminella nätverk som står bakom smuggling.

Tullverket delar polisens bedömning att beslut kommer att behöva tas snabbt på grund av att de kriminella aktörerna ofta har egna säkerhets- och varningssystem.

11.4 Åklagarväsendet

Behovet av att kunna störa pågående brottslighet i digital miljö har blivit alltmer påtagligt i takt med att brottsligheten digitaliseras. Sidor på internet kan liknas vid virtuella brottsplatser, där brottsligheten kan fortgå även efter det att polisen har ingripit mot en enskild individ. I utredningar som rör barnpornografi finns det brottsliga materialet många gånger lagrat, tillgängligt för andra användare. I utredningar som rör narkotikabrott fortsätter handeln ofta på samma sätt som tidigare om inte webbsidans administratörer identifieras och grips. Det är enkelt för vem som helst, även barn, att med hjälp

av internet köpa och få hem otillåtna varor eller att få tillgång till brottsligt övergreppsmaterial. Betalning lämnas ofta i kryptovaluta och verksamheten kan omsätta betydande belopp som går rakt in i den kriminella ekonomin.

I Sverige saknas det i dagsläget medel för att stänga ner en webbsida eller blockera trafiken dit, oavsett om det finns svensk exekutiv jurisdiktion eller inte. Den enda åtgärd som polisen har möjlighet att vidta i dag är att t.ex. på en webbsida informera om att polisen har vetskap om pågående brottslig verksamhet. Polisen har inte rätt att radera ett användarkonto eller övergreppsmaterial som påträffats. Sådana åtgärder måste som huvudregel i stället vidtas av företrädare för plattformen, vilket ofta sker på uppmaning av polisen, men det förutsätter att plattformen samarbetar.

Åklagarmyndigheten anser att myndigheterna behöver kunna störa brottslig verksamhet genom en laglig möjlighet att stänga ner och blockera webbsidor utan legala användningsområden, oavsett om det leder till lagföring eller inte. Bedömningen av om blockering av en webbsida är en lämplig åtgärd bör göras i samråd med förundersökningsledaren. I de fall där det finns möjlighet att spåra administratören bakom en webbsida bör åtgärden vidtas tidigast i samband med tillslag, eftersom administratörens uteblivna aktivitet på marknadsplatsen i samband med att den misstänkte grips generellt utgör central bevisning. I ärenden med sämre prognos för lagföring kan det vara lämpligt att använda åtgärden tidigt, i förebyggande och störande syfte.

Det saknas också laglig möjlighet att ta över administrationen av en webbsida. Misstänktas konton kan inte heller tas över eller brottsliga aktörer stängas ute genom byte av lösenord, eftersom det enligt dagens reglering innebär att polisen begår dataintrång om inte samtycke lämnas av kontoinnehavaren. Att tillåta sådana åtgärder under vissa förhållanden skulle medföra en betydligt ökad förmåga för brottsbekämpande myndigheter att bl.a. kunna identifiera och lagföra högt uppsatta personer inom de kriminella nätverken.

Behovet av att kunna vidta sådana åtgärder som har nämnts och möjligheten att beslagta immateriella tillgångar, bl.a. webbsidor, backupfiler eller konton på sociala medier, har länge påtalats av Åklagarmyndigheten. Även inom Ekobrottsmyndigheten har frågan om beslag av immaterialrättsliga tillgångar diskuterats. I stället för att

åtgärderna ses som en immaterialrättslig fråga, bör de ses i en bredare straffrättslig kontext och i ljuset av RB:s bestämmelser om beslag.

I många andra länder är det kutym att polisen, när den får tillgång till en server, t.ex. genom beslag, lägger ut en s.k. ”splash” som illustrerar att polisen i olika länder samverkat för att slå ut verksamheten. Det görs genom att trafiken på webbsidan dirigeras om till polisens egen webbsida. Åtgärden användes t.ex. när de stora narkotikamarknadsplatserna Silk Road 1 och 2 stängdes ner. Motsvarande åtgärd har även använts vid nedstängning av webbsidor och forum på Darknet som publicerar och sprider övergreppsmaterial.

Flugsvamp 2.0 var den första svenska internationella marknadsplatsen som stängdes ner till följd av en brottsutredning. Åtgärden utfördes av polisen i samband med ett tillslag mot en brottsmisstänkt person, som senare dömdes för att ha administrerat marknadsplatsen.

I det internationella rättsliga samarbetet kommer det ibland förfrågningar från utlandet, bl.a. från FBI i USA, där det begärs att Sverige ska stänga ner webbsidor som säljer varumärkesförfalskningar eller upphovsrättsskyddat material. Det är otillfredsställande att Sverige inte kan bistå med en sådan åtgärd. Ingripanden mot internationella marknadsplatser eller större forum förutsätter som utgångspunkt ett effektivt internationellt samarbete. Eftersom sådana åtgärder är tillåtna i vissa andra länder vidtas de ibland av företrädare för de länderna.

Åklagarmyndigheten understryker särskilt behovet av att säkerställa att inte att all bevisning försvinner om polisen t.ex. skulle få en laglig befogenhet att utföra ett överbelastningsangrepp.

Ekobrottsmyndigheten har ställt sig bakom Åklagarmyndighetens synpunkter.

12 Överväganden om ingripanden i cybermiljö

12.1 Utredningens uppdrag

Av direktiven framgår att det med ökad digitalisering och ny teknik öppnas nya möjligheter för kriminalitet. Kriminella aktörer använder i allt större utsträckning avancerad teknologi för att begå brott. Det handlar inte bara om brott som begås helt digitalt, utan nästan alla brott har i dag en digital komponent.

Brott och brottslig verksamhet i cybermiljö utgör därmed ett växande hot mot både enskilda och den nationella säkerheten. Som exempel kan nämnas att Säkerhetspolisen i sin årsbok för åren 2023 och 2024 konstaterar att Sverige utgör en plattform för främmande makts cyberangrepp. Att hacka privatpersoners enheter och bygga upp kapacitet genom denna typ av infrastruktur möjliggör både cyberangrepp och inhämtning av information. Sett till världen i stort ligger Sverige högt när det kommer till mängden hackad infrastruktur som används för att begå förnekbara cyberangrepp. Totalt under de senaste åren rör det sig om tiotusentals hackade enheter i Sverige.

Utvecklingen har lett till att de brottsbekämpande myndigheterna inte har tillräckligt bra verktyg för att bekämpa brott i cybermiljö. När det gäller sådan brottslighet behöver de brottsbekämpande myndigheterna ändra strategi till att aktivt förhindra, störa och avbryta brott för att minimera skada. Det kan t.ex. handla om att ta sig in i eller etablera sig i en viss digital miljö för att följa den brottsliga verksamheten eller att påverka eller förändra den digitala miljön så att brottsligheten inte kan fortgå. Det finns exempel på andra jämförbara länder som har infört en möjlighet för de brottsbekämpande myndigheterna att bl.a. störa och avbryta pågående brottslighet i

cybermiljö. Sådana regleringar har enligt direktiven visat sig vara ett effektivt verktyg. Utredningen ska därför

- kartlägga och redovisa andra jämförbara länders rättsliga möjligheter att bl.a. störa och avbryta pågående brottslighet i cybermiljö,
- analysera behovet och nyttan av samt föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö, eller vidta andra jämförbara åtgärder i sådan miljö, i syfte att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot sådan brottslighet, och
- lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder.

12.2 Cybermiljön skapar nya utmaningar

12.2.1 En miljö under snabb förändring

Som har framgått av avsnitt 12.2.1 har den snabba tekniska utvecklingen kommit att skapa möjligheter både för kriminella och andra antagonister att hota samhället på nya sätt. De kan utnyttja den anonymitet som internet kan erbjuda för att dölja sina förehavanden, att undkomma upptäckt och att locka andra att delta i olika brottsliga upplägg. Kriminella kan också, bakom anonymitetens skydd, lura personer att investera i obefintliga eller mer eller mindre värdelösa tillgångar eller att överföra ekonomiska medel t.ex. vid romansbedrägerier. Vidare kan de lura personer att klicka på länkar och med hjälp av skadlig kod ta kontroll över deras bankkonton eller exportera den skadliga koden till andra. Särskilt det förhållandet att ekonomiska tillgångar på ett ögonblick kan flyttas från en del av världen till en annan spelar de kriminella i händerna. Det sagda är bara ett axplock av alla nya möjligheter som har öppnats genom den ökade digitaliseringen. Den tekniska utvecklingen innebär att det inte längre är möjligt att angripa den nya typen av kriminalitet med enbart traditionella medel. Det krävs nya verktyg som begränsar möjligheterna att utnyttja digitaliseringen för brottsliga ändamål.

Ett särskilt bekymmer är att utvecklingen av cyberbrottslighet verkar ha fört samman företrädare för främmande makt med tradi-

tionellt kriminella som kan åta sig att låta utföra uppdrag. Gränsen mellan traditionell kriminalitet och samhällsskadlig verksamhet som utförs på uppdrag av främmande makt har därmed i viss utsträckning suddats ut.

12.2.2 Organisation och lagstiftning anpassas till nya behov

I kapitel 10 har utredningen redovisat hur vissa andra länder har börjat anpassa sin lagstiftning till de nya formerna av kriminalitet. Det internationella samarbetet, både inom EU och inom Interpol, utvecklas också fortlöpande för att möta de nya hoten.

Som framgått av kapitel 6–8 har det även i den svenska lagstiftningen tagits olika steg i samma riktning. Det gäller främst inom området för cybersäkerhet. Ett nytt regelverk för cybersäkerhet har införts, där ökade krav ställs på myndigheter, kommuner och företag att ha god cybersäkerhet. Regelverket syftar till att öka medvetenheten om riskerna med brister i cybersäkerheten, att göra det svårare att angripa svenska mål och att skapa en snabb respons på cyberincidenter. En ny organisation som samlar erfarenheter från cyberangrepp och stödjer samhället vid sådana angrepp har också byggts upp (avsnitt 8.1–8.2.2). Förbättrad cybersäkerhet gör Sverige mindre sårbart för cyberangrepp och är därmed en viktig brottsförebyggande åtgärd.

Vidare har framsteg gjorts när det gäller det internationella samarbetet bl.a. genom Budapestkonventionen, som har gett bättre verktyg för att utreda cyberbrott, genom EU-lagstiftningen om digitala tjänster med tillhörande nationell lagstiftning, som syftar till att får bort olagligt innehåll från digitala tjänster genom plattformarnas eller tjänstetillhandahållarnas försorg, och genom TCO-förordningen med tillhörande nationell lagstiftning, som syftar till att hindra spridning av terrorisminnehåll online. I avsnitt 6.4 har också redovisats ett förslag till ny lagstiftning som syftar till att begränsa möjligheterna till onlinerekrytering till brott, genom förelägganden till plattformar om att avlägsna innehåll eller göra det oåtkomligt (prop. 2025/26:276).

EU-lagstiftningen om gränsöverskridande insamling av elektroniska bevis (Effektivare gränsöverskridande inhämtning av elektroniska bevis, prop. 2025/26:147) kommer att ytterligare förbättra

möjligheterna att inhämta sådan elektronisk bevisning i straffrättsliga förfaranden som finns i andra medlemsstater.

Olika lagstiftningsåtgärder har alltså vidtagits för att förbättra möjligheterna att stå emot cyberangrepp och att utreda de cyberbrott som har begåtts. Däremot har polisens möjligheter att ingripa för att störa pågående brottslig verksamhet och att förhindra eller avbryta brott när de begås i digital miljö inte följt med utvecklingen.

12.3 De nuvarande möjligheterna att ingripa

12.3.1 Allmänt om skyldigheten att ingripa mot brott

Polisens uppgift är enligt 1 § polislagen (1984:387) att upprätthålla allmän ordning och säkerhet och att i övrigt tillförsäkra allmänheten skydd och annan hjälp. Det innebär att förhindra att brott begås, att utreda begångna brott, att övervaka den allmänna ordningen och att ingripa för att ställa till rätta när ordningen har störts. Det omfattar en skyldighet att vaka över att allmän ordning och säkerhet inte störs genom brott eller brottslig verksamhet och att ingripa när sådana störningar ändå äger rum. Begreppet allmän ordning och säkerhet omfattar all den egentliga polisverksamheten, som bedrivs av Polismyndigheten och Säkerhetspolisen. I 2 § polislagen förtydligas att Polismyndighetens uppgift bl.a. är att förebygga, förhindra och upptäcka brottslig verksamhet, att ingripa mot störningar och att utreda och beivra brott som hör under allmänt åtal. I 3 § polislagen föreskrivs att Säkerhetspolisens uppgifter bl.a. är att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott och att utreda och beivra bl.a. sådana brott. I 2 kap. 1 § tullbefogenhetslagen (2024:710) föreskrivs bl.a. att Tullverket i sin kontrollverksamhet och brottsbekämpning ska förebygga, förhindra och upptäcka brottslig verksamhet i samband med införsel och utförsel av varor, ingripa vid misstanke om vissa särskilt angivna brott och utreda och lagföra sådana brott.

Enligt 8 § polislagen ska en polisman, som har att verkställa en tjänsteuppgift, under iakttagande av vad som föreskrivs i lag eller annan författning ingripa på ett sätt som är försvarligt med hänsyn till åtgärdens syfte och övriga omständigheter. Måste tvång tillgripas, ska det ske endast i den form och i den utsträckning som behövs för att det avsedda resultatet ska uppnås. Ett ingripande som be-

gränsar någon av de grundläggande fri- och rättigheter som avses i 2 kap. RF får dock inte grundas enbart på den nu aktuella bestämmelsen. En motsvarande reglering finns i 2 kap. 2 § tullbefogenhetslagen och i 2 kap. 1 § kustbevakningslagen (2019:32).

Regleringen i 8 § polislagen ger uttryck för ändamåls-, behovs- och proportionalitetsprinciperna. Det är framför allt den paragrafen som ger polisen rätt att vidta åtgärder mot enskilda. I polislagen regleras också vissa befogenheter för polismän, respektive Polismyndigheten eller Säkerhetspolisen, som får användas oavsett om en förundersökning har inletts eller inte. Exempel på åtgärder som en polisman får vidta, om andra medel är otillräckliga, är att använda våld i syfte att genomföra en tjänsteåtgärd (10 § polislagen), att omhänderta eller avlägsna personer (11–14 §§ polislagen) och att göra husrannsakan i brottsförebyggande syfte (20–20 b §§ polislagen). Vissa åtgärder får Polismyndigheten eller Säkerhetspolisen besluta om, men i brådskande fall får en polisman besluta om åtgärderna. Det handlar t.ex. om att bereda sig tillträde till olika utrymmen för att söka efter vapen (20 b § polislagen). Tullverket har en likartad reglering, enligt vilken en tulltjänsteman har samma befogenheter som en polisman, se bl.a. 8 kap. 6–10 §§ tullbefogenhetslagen.

I förarbetena till polislagen övervägdes om användningen av det som kallades dolda spaningsmetoder skulle regleras. Departementschefen ansåg, i likhet med utredningen, att det inte fanns skäl att särskilt reglera sådana metoder, utan att användningen av dem bör rymmas inom ramen för 8 § polislagen. Departementschefen ställde sig också bakom de principer som utredningen ansåg borde gälla vid användningen av sådana spaningsmetoder, bl.a. följande punkter (Förslag till polislag m.m., prop. 1983/84:111, s. 46 f.).

1. Polisen bör aldrig få begå en kriminaliserad handling för att kunna efterforska eller avslöja ett brott.
2. Polisen bör aldrig få provocera eller annars förmå någon att inleda en brottslig aktivitet.
3. Polisen bör aldrig av spaningsskäl få underlåta att vidta föreskrivna åtgärder mot brott eller en för brott misstänkt person. En annan sak är att vissa åtgärder kan skjutas upp.

Utredningen om stärkt brottsbekämpning genom lagreglering av provokation har konstaterat att de allmänna bestämmelserna om polisens befogenheter enligt polislagen gäller även i underrättelsearbete (Särskilda provokativa åtgärder, SOU 2025:109, s. 61). Enligt utredningens förslag bör dock en provokatör få vidta åtgärder som objektivt sett innefattar självständiga brott men som är kriminaliserade på ett mycket tidigt stadium, motsvarande ett osjälvständigt brott, i syfte att utreda brott eller neutralisera vinsterna från brott. Det rör sig i sådana fall om brott som är ett steg på vägen mot ett ofta allvarligare brott eller där syftet är att tillgodogöra sig vinster från brott, exempelvis finansiering av terrorism eller särskilt allvarlig brottslighet enligt 6 § terroristbrottslagen och grovt penningtvättsbrott enligt 4 och 5 §§ lagen om straff för penningtvättsbrott (SOU 2025:109 s. 154 och 276).

12.3.2 Digitaliseringen har förändrat samhället

Det svenska samhället är i hög grad digitaliserat. Modern teknik innebär många framsteg och nya möjligheter, men tekniken kan samtidigt missbrukas. Kriminella har hittat nya sätt att begå brott med hjälp av framför allt internet och de möjligheter att gömma sig med hjälp av den anonymitet som internet ofta erbjuder. De som ligger bakom brott kan befinna sig långt från brottsplatsen, men ändå uppmuntra och styra andra personer att begå brott för deras räkning. Darknet utnyttjas för att erbjuda försäljning av olagliga varor som narkotika, dopningsmedel, vapen och explosiva varor. Darknet används också för att sprida barnpornografi och material från sexuella övergrepp, men även för att bjuda ut sexuella tjänster. Kriminella tjänster ”annonseras” på olika forum på internet och utförare av brott rekryteras på det sättet. Brottsvinster kan döljas genom att tvättas i kryptovalutor. Till sådana brott som tar sin utgångspunkt i hur internet tekniskt fungerar hör ransomware och överbelastningsangrepp. Sådana brott kan ha till syfte att möjliggöra t.ex. utpressning eller att skada viktiga samhällsintressen. Det sagda är bara ett axplock av all kriminell verksamhet som förekommer på internet. Det visar emellertid att åtgärder mot sådan brottslighet måste anpassas till en rad olika situationer.

12.3.3 Oklart var brotten begås och var bevisningen finns

Ett problem när det gäller dagens lagstiftning är att den digitala miljön – i motsats till den fysiska miljön – inte har några nationella gränser. Det går normalt inte att knyta brott i digital miljö till en viss plats på samma sätt som när det gäller fysiska brott. De brottsbekämpande myndigheternas lagstiftning är däremot i allt väsentligt anpassad till den traditionella fysiska miljön. Det förhållandet att en successiv anpassning av verktygen för brottsutredning har gjorts, bl.a. genom utökade möjligheter att använda hemliga tvångsmedel riktade mot elektronisk kommunikation, förändrar inte den bilden. Samtidigt måste beaktas att brottsbekämpning och de befogenheter som den kräver fortfarande är en nationell angelägenhet.

Genomförandet i svensk rätt av Budapestkonventionen (se avsnitt 7.2) ledde inte till några utökade möjligheter att ingripa mot pågående brott i den digitala miljön. Konventionen syftar, förutom till en tillnärmning av ländernas nationella straffrätt beträffande vissa it-relaterade brott, till att säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser behovet av att utreda och lagföra begångna brott och till att kunna ta tillvara bevisning i elektronisk form och möjliggöra ett snabbt och effektivt internationellt samarbete vid bekämpningen av brotten. Förslaget om effektivare gränsöverskridande inhämtning av elektroniska bevis kommer inte heller att ge de brottsbekämpande myndigheterna de möjligheter att ingripa för att förhindra, störa och avbryta brottslighet som efterfrågas i direktiven. Processrättsliga regler, som underlättar brottsutredning och lagföring, är visserligen viktiga men inte det som behövs för att lösa de nu aktuella problemen.

Till följd av att digital information snabbt kan flyttas, ändras eller tas bort kan det vara mycket svårt för de brottsbekämpande myndigheterna att få tillgång till uppgifter som är vitala för att kunna ingripa mot brott som begås med hjälp av informationssystem. Det gäller både i de fall där gärningsmannen är okänd och i de fall där det finns en känd gärningsman.

Även om det internationella samarbetet på området har förbättrats avsevärt, dels genom att kriminaliseringen av angrepp mot informationssystem numera är mer enhetlig, dels genom utökat internationellt samarbete mot sådana angrepp, kvarstår att internationellt samarbete kan vara både resurskrävande och tidsödande på ett sätt

som försvårar eller omöjliggör de utredningsåtgärder som behövs. Det är inte heller rimligt att svenska myndigheter ska behöva förlita sig på utländska myndigheters möjlighet eller villighet att ingripa.

12.4 Behov och nytta av ny lagstiftning

Utredningens bedömning

Det finns både behov och nytta av att brottsbekämpande myndigheter får befogenhet att ingripa mot brott och brottslig verksamhet i cybermiljö. En sådan reglering får anses innebära ett integritetsintrång som är proportionerligt.

Skälen för utredningens bedömning

Behovet av ny lagstiftning varierar men är generellt sett stort

Som framgått har digitaliseringen av samhället medfört en förhöjd risk för att datorer och elektroniska nätverk används som verktyg för att begå brott. Sådan brottslighet innebär generellt sett också mindre risk för att de som ligger bakom brotten upptäcks och kan lagföras, på grund av de olika tekniker som kan användas i det syftet, t.ex. genom att informationen snabbt flyttas mellan länder och genom totalsträckskryptering av kommunikation och användning av anonymiseringsnätverk. Fler tekniska möjligheter och ökad teknikanvändning skapar nya sårbarheter, som kan utnyttjas av kriminella för att begå brott. Brottslighet i form av olika typer av digitala angrepp utgör ett växande samhällshot. Vissa angrepp kan riktas mot Sverige från främmande makt och avse exempelvis myndigheters och kommuners nätverk och annan samhällsviktig digital infrastruktur. Brottslighet i digital miljö utgör även ett allt större hot mot enskilda genom t.ex. utpressningsangrepp mot företag och privatpersoner, omfattande bedrägerier, olika former av sexuell exploatering av barn och rekrytering av barn och unga till kriminella nätverk.

De brottsbekämpande myndigheterna har, var och en utifrån sitt uppdrag, lyft olika aspekter på behovet av nya verktyg för att komma till rätta med brott som begås med hjälp av internet (se kapitel 11).

Polismyndigheten har framhållit att kvalificerade cyberbrott som ransomware, informationsstölder, överbelastningsangrepp och fenomenet crime as a service vållar stor samhällsskada. Myndigheten har särskilt lyft riskerna att digital information snabbt kan hamna utom räckhåll för nationella myndigheter och de krav på snabba ingripanden som det medför. Polismyndighetens uppgift att ingripa gäller oavsett i vilken miljö ett brott begås. Att myndigheten i dag saknar lagstöd för att kunna ingripa mot brott och brottslig verksamhet i digital miljö är otillfredsställande och riskerar enligt myndigheten att urholka allmänhetens förtroende för rättsväsendet.

Säkerhetspolisen har påpekat att internet gör det möjligt för främmande makt att dels i större utsträckning försvåra att deras verksamhet i Sverige kan kartläggas, dels genom dataintrång via internet hämta in skyddsvärd information på ett relativt enkelt och riskfritt sätt när som helst under dygnet. Risken för radikalisering genom material på internet har också framhållits. Behovet av att kunna ingripa i digital miljö har enligt myndigheten successivt ökat.

Tullverket har framhållit att den ökade mängden av beslag i post- och kurirflödet av narkotika, vapen, explosiva varor och andra varor som inte får föras in i Sverige utan tillstånd till stor del har sitt ursprung i försäljning av varorna på illegala digitala marknadsplatser. Smugglingen medför stor samhällsskada och försäljningssättet gör det svårt att identifiera vem eller vilka som ligger bakom smugglingen. Det är därmed svårt att vidta adekvata åtgärder mot brotten.

Åklagarmyndigheten har lyft fram behovet av att kunna förhindra att brottsligt material, t.ex. rörande övergrepp på barn, finns kvar på internet sedan de misstänkta har gripits och lagförts. Enligt myndigheten är det också viktigt att kunna förhindra fortsatt handel med narkotika på digitala marknadsplatser när någon har lagförts.

De brottsbekämpande myndigheterna är eniga om att de nuvarande möjligheterna att ingripa mot brott som begås i digital miljö är alltför små och att det därför krävs ny lagstiftning för att de ska kunna fullgöra sina uppdrag.

Brott av det nu aktuella slaget kan enligt utredningens mening orsaka betydande skada både materiellt och personligt för de som utsätts för brotten, eftersom i stort sett alla verksamheter numera på ett eller annat sätt är beroende av digitala tjänster. Den straffrättsliga lagstiftningen har successivt anpassats till att brott inte bara begås i den fysiska miljön utan även i den digitala. Den del av lagstiftningen

som syftar till att ingripa mot brott är dock alltjämt i allt väsentligt inriktad på den fysiska miljön.

Att cyberbrott eller cyberrelaterade brott kan förhindras – eller i vart fall att brottslig verksamhet av det slaget kan störas och att pågående brott i digital miljö kan avbrytas – är ett tungt vägande samhällsintresse. Det gäller särskilt mot bakgrund av de allvarliga konsekvenser sådana brott kan få både för samhället i stort och för enskilda. Det kan gälla allt från störning av försörjningen av el, vatten eller annan samhällsviktig infrastruktur till sexuella övergrepp mot barn, omfattande bedrägerier mot skyddslösa äldre eller cyberspionage. Att kunna ingripa mot sådan brottslighet, väger tungt även ur ett brottsofferperspektiv. Ju allvarligare brott det är fråga om, desto starkare gör sig intressena gällande.

Finns det några alternativa lösningar?

Cyberbrott, cyberrelaterade brott och den framväxande internationella brottsligheten i digital miljö, framför allt den alltmer systemhotande brottslighet som brukar kallas crime as a service, behöver kunna bekämpas effektivt. Ingripanden mot brott och brottslig verksamhet i fysisk miljö skiljer sig emellertid väsentligt från ingripanden i digital miljö. Det ställs andra krav på lagstiftningen för att sådana ingripanden ska vara möjliga, eftersom straffbestämmelsen om dataintrång har ett brett tillämpningsområde och inte gör något undantag för brottsbekämpning. De brottsbekämpande myndigheterna saknar i dag lagstöd för att kunna ingripa i digital miljö, vilket innebär att de inte har de verktyg som krävs för att kunna fullgöra sina uppdrag.

Utredningen bedömer därför att de brottsbekämpande myndigheterna behöver ges rättsliga möjligheter att ingripa mot brott och brottslig verksamhet i cybermiljö och att det inte finns något alternativ till ny lagstiftning.

Nyttan

Befogenheter för de brottsbekämpande myndigheterna att ingripa i den digitala miljön skulle ge nya verktyg i brottsbekämpningen. Om sådana befogenheter införs kan det, mot bakgrund av hur brottslig-

heten har utvecklats, med fog förväntas leda till ökad samhällsnytta. Nya befogenheter kommer att innebära att de brottsbekämpande myndigheterna, på ett betydligt effektivare sätt än i dag, kan förhindra att brott i digital miljö begås, störa brottslig verksamhet och avbryta pågående brott i sådan miljö. Den tekniska utvecklingen kan dessutom förväntas fortsätta och – även om det är en oönskad effekt – skapa nya möjligheter att begå brott. Brott och brottslig verksamhet som helt eller delvis utförs med hjälp av digitala verktyg behöver kunna motverkas digitalt, för att brottsbekämpningen ska vara effektiv och avhålla personer från att begå brott. Det är viktigt att Sverige har en adekvat lagstiftning och inte riskerar att bli måltavla för internationell brottslighet eller för angrepp från främmande makt. Nya befogenheter som ger möjlighet att ingripa mot sådan brottslighet bör därför enligt utredningens mening kunna få stor praktisk nytta.

Integritetsintrånget

Den typ av ingripanden som det kan bli fråga om kommer, som påpekats i andra lagstiftningsärenden, oundvikligen att påverka enskildas integritet. Varje befogenhet för staten att bereda sig tillträde till personlig information om enskilda, oavsett om det görs med tvång eller inte, liksom varje utnyttjande av en sådan befogenhet, leder till intrång i den personliga integriteten (Hemliga tvångsmedel mot allvarliga brott, SOU 2012:44, s. 32 och 480). Olika former av ingripanden kan dock förväntas få varierande påverkan. Avgörande för hur stort integritetsintrånget blir bör som utgångspunkt vara karaktären och omfattningen av dels de uppgifter som ingripandet avser, dels det informationssystem, eller delar av informationssystem, som ingripandet avser. Vidare bör varaktigheten av åtgärden ha betydelse för hur stort integritetsintrånget blir.

Att myndigheter bereder sig tillgång till informationssystem som används av enskilda kan i vissa fall leda till intrång som för den enskilde har likheter med det intrång som användning av hemliga tvångsmedel medför. I andra fall kan sådana ingripanden medföra mer begränsade integritetsintrång.

En särskild aspekt är att vissa informationssystem eller delar av dem, t.ex. vissa användarkonton, har som enda ändamål att möjliggöra eller främja allvarlig eller systematisk brottslighet. När det gäl-

ler sådana informationssystem får det integritetsintrång som kan följa av att en myndighet ingriper mot verksamheten enligt utredningens mening generellt betraktas som acceptabla. Det gäller t.ex. marknadsplatser på Darknet som bjuder ut narkotika eller andra förbjudna föremål till försäljning eller som syftar till att underlätta sexuella övergrepp mot barn på distans.

Integritetsintrånget får även anses vara mera begränsat i de fall där en nätansluten enhet, som t.ex. en uppkopplad bevakningskamera, har angripits och den utan ägarens vetskap utnyttjas i ett anonymiseringsnätverk. I de fallen kan ett ingripande snarare ses som positivt av den som äger eller använder enheten, om utnyttjandet av enheten kan stoppas.

Vissa ingripanden kan förväntas leda till integritetsintrång av tillfällig karaktär, om uppgifterna som åtgärden riktas mot är möjliga att återställa. Andra åtgärder kan leda till större integritetsintrång om de är av oåterkallelig karaktär. Det måste givetvis beaktas när lagstiftningen utformas. I de flesta fall bör ingripandena vara kortvariga, men det kan också finnas fall där ingripandet varar längre.

De olika åtgärder som kan aktualiseras vid ingripanden mot cyberbrott kan alltså variera avsevärt i fråga om vilka konsekvenser de får för enskilda. Hur stort det samlade integritetsintrånget av den nya regleringen förväntas bli återkommer utredningen till.

Proportionalitet

Olika former av ingripanden bör kunna komplettera varandra. Den minst ingripande åtgärden bör som utgångspunkt användas i första hand. För att en reglering som ger de brottsbekämpande myndigheterna möjlighet att ingripa mot den aktuella brottsligheten ska anses vara proportionerlig bör det emellertid ställas upp olika begränsningar för sådana åtgärder. Utredningen återkommer till det.

Slutsatser

Vid en samlad bedömning anser utredningen att de brottsbekämpande myndigheternas behov av att kunna ingripa mot brott och brottslig verksamhet i den digitala miljön väger tyngre än de nackdelar som sådana ingripanden kan föra med sig. Ingripanden kan för-

väntas bli effektiva verktyg för att förhindra cyberbrott och även för att störa brottslig verksamhet i digital miljö och avbryta brott i sådan miljö. Samhällsintresset av att brottsbekämpande myndigheter har rättsliga möjligheter att ingripa mot sådana brott och cyberrelaterade brott är stort och det saknas alternativa tillvägagångssätt. Utredningen bedömer därför att det är proportionerligt att ge myndigheterna nya befogenheter för att motverka brott och brottslighet som använder digitala informationssystem som ett medel.

12.5 Det behövs ny lagstiftning

Utredningens bedömning

Den befintliga lagstiftningen är otillräcklig för att tillgodose de brottsbekämpande myndigheternas behov av att kunna ingripa mot brott och brottslig verksamhet i digital miljö. Det behövs därför ny lagstiftning som fyller det behovet.

Skälen för utredningens bedömning

Regleringen om dataintrång hindrar ingripanden

Ett särskilt problem är att de åtgärder som de brottsbekämpande myndigheterna skulle behöva vidta för att kunna ingripa mot brott i den digitala miljön normalt förutsätter handlande som är kriminaliserat som dataintrång. Straffbestämmelsen om dataintrång finns i 4 kap. 9 c § brottsbalken (se avsnitt 5.1). Den har utformats för att svara mot kraven både i Europaparlamentets och rådets direktiv 2013/40/EU den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF och i Budapestkonventionen.

Det som behövs för att brottsbekämpande myndigheter ska kunna upptäcka, avbryta och förhindra brott och brottslighet i den digitala miljön är bl.a. att myndigheterna ges rätt att bryta systemskydd för att bereda sig tillgång till uppgifter i informationssystem. Myndigheterna kan också behöva föra in nya uppgifter, ändra befintliga uppgifter eller blockera de uppgifter som behandlas i syste-

men. Eftersom åtgärder av det slaget, liksom vissa andra åtgärder, som att radera digital information, är kriminaliserade som dataintrång krävs det en reglering som ger ett positivt lagstöd för att brottsbekämpande myndigheter ska få vidta dem.

Ingrepp i privatlivet kräver lagstöd

Ett skäl till att det krävs lagstöd för nya befogenheter för att kunna ingripa mot brott i digital miljö är det skydd som var och en enligt artikel 8 i Europakonventionen har rätt till för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Offentliga myndigheter får inte inskränka de rättigheterna annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bl.a. med hänsyn till statens säkerhet och den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd för andra personers fri- och rättigheter. Som tidigare har nämnts gäller numera Europakonventionen som svensk lag (avsnitt 3.3). Lag eller annan föreskrift får enligt 2 kap. 19 § RF inte meddelas i strid med Sveriges åtaganden enligt Europakonventionen.

Enligt 2 kap. 6 § andra stycket RF har var och en skydd gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. De grundläggande rättigheterna i 2 kap. RF får begränsas endast genom lag och för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får enligt 2 kap. 20 och 21 §§ RF aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen.

Det behövs nya verktyg

Slutsatsen av det sagda är att den nuvarande lagstiftningen inte tillåter de åtgärder som de brottsbekämpande myndigheterna behöver kunna vidta för att förhindra, störa och avbryta den brottslighet som förekommer i digital miljö. Det främsta skälet är att åtgärderna i fråga uppfyller rekvisiten för brottet dataintrång, samtidigt som den befintliga regleringen av myndigheternas befogenheter inte tillåter något undantag från den regleringen. Därför behöver de brottsbe-

kämpande myndigheterna nya verktyg. Den reglering som krävs ska ha lagform.

Det bör framhållas att syftet med en ny reglering – i motsats till straffprocessuella tvångsmedel – inte är att hämta in och bearbeta information för att kunna utreda och lagföra brott och inte heller att ge underlag till och berika underrättelseverksamhet. I stället bör syftet vara att möjliggöra ingripanden på ett tidigt stadium för att kunna förhindra och – om det inte är möjligt – avbryta brott i digital miljö och begränsa verkningarna av brottsligheten.

13 En ny lag om polisiära ingripanden i cybermiljö

13.1 En ny lag bör införas

13.1.1 En ny lag är det bästa alternativet

Utredningens förslag

Det ska införas en ny lag om ingripanden i cybermiljö.

Skälen för utredningens förslag

Regleringen passar inte in i någon befintlig lagstiftning

En ny lagstiftning om ingripanden i cybermiljö kommer att behöva behandla en rad olika frågor, från hur tillämpningsområdet bör avgränsas och vilka åtgärder som ska vara tillåtna, till vem som bör besluta om sådana ingripanden och vad som bör gälla för verkställigheten av dem. Det handlar således inte bara om några få paragrafer.

Den första frågan som väcks är om en ny reglering kan inlemmas i någon befintlig lagstiftning. Ett förslag som har nämnts i sammanhanget är polislagen. För att kunna ta ställning till om en ny reglering har sådana beröringspunkter med någon existerande författning att den lämpligen bör placeras där behöver det först diskuteras vilken typ av lagstiftning som krävs.

En viktig fråga är om ingripanden bör förbehållas situationer där det finns förutsättningar för att inleda förundersökning eller om det bör vara möjligt att ingripa även tidigare. Den frågan måste ses i ljuset av vad som är syftet med ingripandena. Syftet med den nya regleringen ska – enligt direktiven – vara att kunna förhindra, störa och

avbryta brott i digital miljö. Ändamålet med ingripandena bör alltså inte vara att samla in information som kan användas för brottsutredning och lagföring, utan att störa och avbryta brottslighet och därigenom, om möjligt, förhindra att brott begås.

För att en ny reglering ska bli tillräckligt effektiv bör den enligt utredningens mening inte begränsas till enbart de situationer där det finns förutsättningar för att inleda förundersökning. Det ska således inte vara fråga om en ny kategori av åtgärder som är avsedda att användas för att utreda och lagföra brott. Det innebär att en ny reglering inte bör placeras i RB.

Preventiva tvångsmedel får enligt särskilda lagar användas i underrättelseverksamhet, i syfte att inhämta information för att kunna förhindra eller, i fråga om lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen), förebygga, förhindra och upptäcka brottslig verksamhet. I förlängningen är avsikten med de lagarna att brott som upptäcks ska utredas och, om möjligt, lagföras. Syftet med sådana tvångsmedel är alltså delvis detsamma som enligt direktiven ska uppnås, men den befintliga lagstiftningen skulle behöva omarbetas väsentligt för att även ingripanden i digital miljö skulle kunna regleras där. I motsats till det som gäller för brottsutredning och lagföring finns det inte heller någon generell lagstiftning som reglerar underrättelseverksamhet (se Effektivare verktyg för att bekämpa brott av unga lagöverträdare, SOU 2024:93, s. 689 f.). Om så hade varit fallet hade den nya regleringen eventuellt kunnat placeras där.

En möjlighet att ingripa mot brott i digital miljö måste kunna fungera både på underrättelsestadiet, för att upptäcka och förhindra brott eller störa eller avbryta brottslig verksamhet, och på utredningsstadiet, för att myndigheterna ska kunna agera mot pågående brott. Det finns med andra ord enligt utredningens mening inte förutsättningar att placera en ny lagstiftning i någon befintlig lagstiftning som reglerar brottsbekämpning.

Utredningen anser inte heller, av flera skäl, att en placering av den nya regleringen i polislagen är lämplig. Polislagen gäller visserligen i all polisverksamhet, men den har sin tyngdpunkt främst i polisens uppgift att upprätthålla allmän ordning och säkerhet. De befogenheter som regleras i lagen är i hög grad knutna till den fysiska miljön. Den brottsbekämpande verksamheten regleras i huvudsak i annan

lagstiftning, framför allt RB med tillhörande författningar, även om t.ex. våldsanvändningen regleras i polislagen. En ändring av polislagen skulle få konsekvenser även för annan polisiär verksamhet än den – mycket begränsade – del av polisverksamheten som nu är aktuell. Det skulle kräva överväganden som inte är möjliga att göra inom ramen för den här utredningen. Dessutom skulle det krävas särskild lagstiftning om någon annan myndighet än Polismyndigheten och Säkerhetspolisen ska ges nya befogenheter.

En ny lagstiftning kan vidare behöva tidsbegränsas. Även av det skälet är en placering i befintlig lagstiftning olämplig.

Slutsatsen är alltså att det bör införas en helt ny lag.

Möjligheten att ingripa bör gälla i cybermiljö

Frågan är hur lagens tillämpningsområde bör avgränsas, för att tillämpningsområdet inte ska bli alltför snävt. En möjlighet kan vara att ange att lagen är tillämplig i cybermiljö. Med cybermiljö brukar avses en övergripande miljö eller domän där digital information skapas, bearbetas, kommuniceras och lagras. Cybermiljö, eller cyberrymden, kan också beskrivas som den miljö som bildas av fysiska och icke-fysiska komponenter för att lagra, modifiera och utbyta data med hjälp av datornätverk (se The Tallinnmanual 2.0 on the international law applicable to cyber operations, 2017, s. 614).

Begreppet cybermiljö omfattar alltså all form av verksamhet och kommunikation som äger rum via ihopkopplade informationssystem. Det inkluderar digitala miljöer i form av webben, sociala medier och andra digitala plattformar, men även teknisk infrastruktur som datorer, servrar, lagringstjänster, nätverk och andra digitala system som utgör grunden för den digitala miljön. Cybermiljön består alltså av digitalt skapade och tekniskt sammanlänkade utrymmen där information utbyts, kommunikation sker och händelser initieras – utan att de nödvändigtvis är bundna till ett visst geografiskt territorium eller en fysisk plats. Miljön skiljer sig därigenom från den fysiska miljön genom avsaknaden av traditionella gränser.

Utredningen anser att ett lämpligt sätt att precisera var ingripanden bör få äga rum med stöd av den nya lagstiftningen kan vara att använda begreppet cybermiljö.

13.1.2 Ingripanden mot både brott och brottslig verksamhet

Utredningens förslag

Rätten att ingripa ska avse både brott och brottslig verksamhet.

Skälen för utredningens förslag

Ingripanden mot verksamhet i cybermiljö bör som nämnts i avsnitt 12.3.2 kunna avse en mängd olika företeelser. På samma sätt som vid ett ingripande mot brott i den fysiska miljön kan det långt ifrån alltid förutses vilka kriminaliserade företeelser som ingripandet kan komma att avslöja. Möjligheten att ingripa bör därför gälla oavsett om det är fråga om ett tydligt identifierbart brott eller om ingripandet riktar sig mot ett handlande som på goda grunder kan antas vara brottsligt, men där det saknas klarhet i exakt vilket eller vilka brott det kan vara fråga om. Det sistnämnda är typiskt för underrättelseverksamhet. För att den nya regleringen ska kunna bli tillräckligt effektiv för att förhindra brott bör den därför enligt utredningens mening inte begränsas till enbart ingripanden där det finns förutsättningar att inleda förundersökning, utan bör även omfatta ingripanden på underrättelsestadiet. Den nya regleringen bör således kunna tillämpas på både brott och brottslig verksamhet.

Vad som avses med begreppet brott behöver inte diskuteras närmare. Däremot är det inte lika självklart vad som avses med begreppen brottslighet och brottslig verksamhet. Uttrycken används i flera olika sammanhang i lagstiftningen, men med lite olika betydelse. Inom straffrätten används uttrycket brottslighet främst för att beteckna flera brott (se t.ex. 8 kap. 4 § och 29 kap. 1 § brottsbalken). I förarbetena till straffbestämmelsen om involverande av underårig i brottslighet i 16 kap. 5 a § brottsbalken framhålls att brottslig verksamhet är ett vidare begrepp än brott och tar sikte på en viss typ av brottslighet som inte behöver vara närmare preciserad i fråga om omfattning och detaljer. Brottslig verksamhet omfattar såväl brottslighet vid ett enda tillfälle som flera brott som hänger samman, men även enstaka brott inom ramen för en verksamhet som bedrivs i mer eller mindre organiserade former (Skärpta straff för brott i kriminella nätverk, prop. 2022/23:53, s. 145). Inom processrätten används begreppen ibland på samma sätt som i brottsbalken. Men i huvudsak

används begreppet brottslig verksamhet för att skilja mellan de två huvudgrenarna inom brottsbekämpningen, nämligen underrättelseverksamhet och förundersökning. Det används bl.a. i brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Som tidigare har nämnts används begreppet brottslig verksamhet även i polislagen. Det används också i förordningen (2022:1719) med instruktion för Säkerhetspolisen och i tullbefogenhetslagen. Det är alltså ett inarbetat begrepp.

I detta sammanhang avser utredningen med brottslig verksamhet en inte närmare preciserad verksamhet som innefattar flera kriminaliserade handlingar. Det innebär att handlingarna inte tillsammans, eller var och en för sig, behöver uppfylla rekvisiten för ett visst konkret brott, utan endast att de är tecken på någon identifierbar form av brottslighet. Det kan exempelvis vara viss ekonomisk brottslighet, förmögenhetsbrottslighet eller sexualbrottslighet.

Mot den nu angivna bakgrunden bör lagens tillämpningsområde avgränsas genom att det anges att regleringen gäller både brott och brottslig verksamhet i cybermiljö.

13.1.3 Vilka myndigheter bör kunna tillämpa lagen?

Utredningens förslag

Lagen ska ge Polismyndigheten, Säkerhetspolisen och Tullverket befogenheter att ingripa mot brott och brottslig verksamhet i cybermiljö.

Skälen för utredningens förslag

Eftersom det är fråga om en lagstiftning vars syfte är att myndigheter ska kunna ingripa mot brott bör den nya regleringen tillämpas av myndigheter som dels har till uppgift att bekämpa de typer av brott som kan vara aktuella i sammanhanget, dels har nödvändiga rättsliga och praktiska förutsättningar för att kunna ingripa på ett effektivt sätt, ytterst genom sin rätt att använda våld. Det bör också vara myndigheter som har en naturlig anknytning till de brott som begås i cybermiljö. Det innebär att det i praktiken i första hand är fråga om

Polismyndigheten och Säkerhetspolisen. Även Tullverket lever upp till de kraven, medan däremot Kustbevakningen har sina huvudsakliga uppgifter i den fysiska miljön och därför inte bör omfattas av regleringen. För Skatteverkets del kan konstateras att myndigheten har mycket begränsade befogenheter för brottsbekämpning jämfört med övriga myndigheter med det uppdraget och därför inte heller bör omfattas av regleringen. Det bör alltså framgå av den nya lagen att de myndigheter som får ingripa med stöd av lagen ska vara Polismyndigheten, Säkerhetspolisen och Tullverket.

Det kan inte uteslutas att andra myndigheter än de nu nämnda i framtiden kan behöva tillämpa den nya regleringen, med tanke på den snabba tekniska utvecklingen och förändringarna i övrigt som kännetecknar brottsligheten i cybermiljö, men i dagsläget finns det inte något underlag för det.

13.1.4 Lagens benämning

Utredningens förslag

Lagen ska benämnas lag om polisiära ingripanden i cybermiljö.

Skälen för utredningens förslag

Lagen bör benämnas lag om polisiära ingripanden i cybermiljö. Den kommer framför allt att tillämpas av Polismyndigheten och Säkerhetspolisen. Det förhållandet att lagen även föreslås tillämpas av Tullverket hindrar enligt utredningens mening inte att ingripandena betecknas som polisiära, eftersom Tullverket inom sitt verksamhetsområde i princip har samma befogenheter att ingripa mot brott och brottslig verksamhet som Polismyndigheten. Det kan även anmärkas att lagen (2023:474) om polisiära befogenheter i gränsnära områden reglerar befogenheter inte bara för polismän utan även för kustbevakningstjänstemän och tulltjänstemän.

Det är en fördel om benämningen på en lag är kort. Utredningen har övervägt om även ordet ”befogenheter” bör ingå i rubriken, men anser att det inte skulle tillföra något, eftersom det ligger i sakens natur att det följer vissa befogenheter med rätten att ingripa. Även

frågan om brott och brottslig verksamhet bör ingå i lagens rubrik har övervägts men har förkastats av i huvudsak samma skäl.

13.2 Lagens tillämpningsområde

Utredningens förslag

Begreppet informationssystem ska användas för att avgränsa tillämpningsområdet.

Skälen för utredningens förslag

Allmänt om informationssystem

I straffbestämmelsen om dataintrång begränsas det straffbara området genom att den olovliga åtgärden ska avse uppgifter avsedda för automatiserad behandling. Sådana uppgifter hanteras av digitala informationssystem. I det ingår hårdvara, mjukvara, data och nätverkskomponenter som samverkar för att samla in, lagra, bearbeta eller överföra uppgifter utan kontinuerlig manuell styrning.

I EU-direktivet om angrepp mot informationssystem, som bestämmelsen om dataintrång delvis genomför, definieras informationssystem i artikel 2 som en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar datorbehandlingsbara uppgifter samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av en apparat eller en grupp av apparater för att de ska kunna drivas, användas, skyddas och underhållas.

I 1 kap. 2 § cybersäkerhetslagen (2025:1506), som delvis genomför NIS 2-direktivet, definieras nätverks- och informationssystem som en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller digitala uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av ett elektroniskt kommunikationsnät som avses i 1 kap. 7 § LEK eller någon av nyssnämnda funktioner för att de ska kunna användas, skyddas och underhållas.

När lagen (2020:62) om hemlig dataavläsning infördes konstaterade regeringen att flera remissinstanser var kritiska till användningen av begreppet informationssystem, vilket utredningen hade föreslagit. Skälet till det var att det begreppet redan användes i andra sammanhang på ett sätt som inte stämde överens med hur det användes i den föreslagna lagen om hemlig dataavläsning. Regeringen ansåg att begreppet ”avläsningsbart informationssystem” bättre beskrev det som avsågs (Hemlig dataavläsning, prop. 2019/20:64, s. 104). I förarbetena utvecklades inte närmare vad som avsågs med avläsningsbart informationssystem.

Begreppet informationssystem bör användas

Ett sätt att avgränsa tillämpningsområdet för den nya lagen är att knyta det till begreppet informationssystem. Det begreppet används inom olika lagstiftningsområden, men innebörden av begreppet kan variera något.

Utredningen anser att det förhållandet att begreppet informationssystem används på något olika sätt i lagstiftning som har skilda ändamål inte hindrar att det används i detta sammanhang. Användningen av ett visst begrepp måste alltid anpassas till lagstiftningens ändamål och läsas i ljuset av vilken roll det spelar i just det aktuella fallet. Eftersom informationssystem är ett vedertaget begrepp när det gäller hantering av digital information och det enklast sammanfattar det centrala för den nu aktuella lagstiftningen bör det användas. Utredningen anser därför att begreppet informationssystem är lämpligt för att avgränsa tillämpningsområdet och tydliggöra att ingripandena endast bör få avse brott och brottslig verksamhet i cybermiljö.

Någon definition av vad som avses med informationssystem anser utredningen inte vara nödvändig. En sådan definition skulle kunna leda till en teknisk begränsning som varken är avsedd eller lämplig. Genom att lagstiftningen bara är tillämplig i cybermiljö utesluts dock alla informationssystem som enbart är manuella.

Det ligger i sakens natur att det måste finnas någon form av information som gör att det aktuella informationssystemet kan identifieras, för att ett ingripande ska kunna göras. Däremot är det långt ifrån säkert att informationssystemet kan knytas till en fysisk person

på det sätt som krävs i en förundersökning. Någon sådan koppling bör inte heller krävas.

Det bör redan här framhållas att de ingripanden som kan bli aktuella mycket sällan kommer att behöva avse ett helt informationssystem som sådant. Det kan förutsättas att ingripandena i de flesta fall kommer att avse en begränsad mängd uppgifter som behandlas i ett informationssystem, eller i en särskilt avgränsad del av systemet, som t.ex. en viss katalog eller vissa enskilda datafiler i ett användarkonto. På samma sätt som vid ingripanden i fysisk miljö går det dock inte att på förhand bedöma vad ingripandet kan resultera i. Hänsyn måste dock alltid tas till risken för att ovidkommande personer eller enheter drabbas, vid bedömningen av om ett ingripande i ett visst informationssystem är proportionerligt. Behovet av ingripande kan vara lika stort oberoende av hur och var uppgifterna lagras, medan integritetsintrånget kan variera. Ingripandena bör emellertid i många fall kunna begränsas till t.ex. användarkonton till kommunikations- eller lagringstjänster eller enstaka hemsidor på en server.

13.3 Frågor om jurisdiktion

13.3.1 Bakgrund

Polisens ingripanden i fysisk miljö grundas dels på skyldigheten att upprätthålla allmän ordning och säkerhet, dels på skyldigheten att ingripa mot brott. Tullverket har en liknande skyldighet att ingripa vid misstanke om brott inom myndighetens verksamhetsområde. Som beskrivits förutsätter det inte någon närmare kunskap om vad ingripandet kan komma att utmynna i. Däremot är det en självklarhet att ingripanden endast kan göras i situationer där Sverige har territoriell behörighet eller på annan grund anses ha rätt att ingripa mot brott. Därmed begränsas behörigheten till situationer där ett eventuellt brott ligger under svensk domsrätt.

Cybermiljön är ett utmanande område för rättsordningen. Det är en värld där anonymisering och avsaknaden av fysiska gränser riskerar att underminera de traditionella jurisdiktionsprinciperna. Gärningsman, brottsoffer, data och tekniska resurser befinner sig inte sällan i olika jurisdiktioner. Förhållandena kan dessutom förändras snabbt när data flyttas med hjälp av molntjänster, proxyservrar och anonymiseringsnoder. Det ställer krav på en annan syn på rättslig kon-

text, där cybermiljön i högre grad kan likställas med t.ex. rymden i det avseendet att båda saknar traditionella gränser. Det finns ingen rättskälla som tydligt skiljer cybermiljön från den fysiska miljön i jurisdiktionshänseende. Cybermiljön omfattas av folkrättens ramar, även om tillämpningen kan vara tekniskt och politiskt utmanande.

Brottslighet i cybermiljö kan innebära antingen att användning av den miljön är en direkt förutsättning för att ett brott ska kunna begås, exempelvis ett överbelastningsangrepp, eller enbart är ett medel för att begå ett brott som lika gärna kunde ha begåtts i fysisk miljö, t.ex. bedrägeri, utpressning eller sexuella övergrepp mot barn. Vid brott som begås med hjälp av informationssystem kan, som nyss nämnts, gärningsmannen befinna sig i en helt annan del av världen än där själva brottet äger rum. Den nya lagen förutsätter inte att det finns någon identifierad gärningsman utan endast ett identifierat informationssystem. Det är nämligen långt ifrån säkert att det informationssystem som utnyttjas kan knytas till en fysisk person på det sätt som krävs i en förundersökning. Det är inte heller givet att det ens vid själva ingripandet går att klarlägga om ett eller flera informationssystem är inblandade och vilka brott som har begåtts eller pågår med hjälp av informationssystemet. I många fall kan dessutom brott begås eller brottslig verksamhet bedrivas helt eller delvis med hjälp av olika informationssystem som är spridda runt om i världen. Det kan vara noder som ingår i ett anonymiseringsnätverk som inte är möjliga att identifiera och lokalisera, vilket gör att det inte är möjligt att avgöra från vilket informationssystem som ett cyberangrepp ursprungligen härrör.

Eftersom ett viktigt syfte med den nya lagen är att kunna ingripa redan innan ett konkret brott har begåtts, eller att kunna störa och avbryta brottslig verksamhet, ligger det i sakens natur att inte alla omständigheter som konstituerar ett brott är kända för den brottsbekämpande myndigheten vid ingripandet. För att ett ingripande enligt den nya lagen ska kunna riktas mot ett visst informationssystem krävs det emellertid tillräcklig information för att kunna identifiera systemet. Dessutom bör det krävas någon form av anknytning till Sverige. Den anknytningen kan utformas på olika sätt.

13.3.2 Allmänt om svensk domstols behörighet i brottmål

I 2 kap. brottsbalken regleras när svensk domstol är behörig att döma över ett visst konkret brott. Innehållet där är allmängiltigt och gäller för alla typer av brott, om inte något annat framgår. Kapitlet har utformats mot bakgrund av de folkrättsliga anknytningsprinciperna (Aggressionsbrottet i svensk rätt och svensk straffrättslig domsrätt, prop. 2020/21:204, s. 87). Regleringen i 2 kap. brottsbalken utgör i sin tur grunden för när brottsbekämpande myndigheter får ingripa mot brott och för brottsutredning och lagföring.

Huvudregeln i 2 kap. 1 § första stycket brottsbalken ger uttryck för rättsgrundsatsen att svensk domstol är behörig att döma över brott som har begåtts i Sverige, den s.k. territorialitetsprincipen (NJA II 1962 s. 55 och NJA II 1973 s. 38).

Enligt 2 kap. 1 § andra stycket brottsbalken ska ett brott anses ha begåtts i Sverige om gärningsmannen handlade här. Bestämmelsen bygger på den s.k. ubikvitetsprincipen, som innebär att det är tillräckligt att någon del av brottet har begåtts i Sverige för att det ska kunna lokaliseras hit.

Ett brott anses vidare anses ha begåtts i Sverige om det för straffansvar krävs att gärningen har medfört en viss effekt, under förutsättning att effekten inträdde i Sverige eller, vid försök, sannolikt skulle ha inträtt här. Regleringen bygger på den s.k. effektprincipen. Ett brott som förutsätter en viss effekt anses ha begåtts i Sverige om effekten inträdde här, även om den brottsliga handlingen begicks utomlands. En gärning som har påbörjats utanför Sverige anses alltså vara fullbordad här i landet om effekten av handlingen har uppkommit i Sverige (Agneta Bäcklund m.fl., Brottsbalken, En kommentar, JUNO, 2025-11-18, kommentaren till 2 kap. 1 §). Det krävs att effekten har ett direkt samband med den brottsliga gärningen. Med det avses inte endast effekter som innebär att fullbordanspunkten i straffrättslig mening inträffat i Sverige, utan också omedelbara effekter av ett brottsligt handlande. Sådana följder av ett brott som saknar omedelbart samband med rekvisiten för ett brott påverkar inte brottets lokalisering, dvs. var brottet ska anses ha begåtts (Högsta domstolens dom den 30 december 2025 i mål B 5546–24, ”Internetförtalet”, p. 14).

Enligt 2 kap. 1 § tredje stycket brottsbalken ska ett brott som utgör medverkan till någon annans brott anses ha begåtts i Sverige om

den medverkande handlade här. Om gärningsmannens brott anses ha begåtts i Sverige, anses den medverkandes brott också ha begåtts här.

I 2 kap. 3 § brottsbalken regleras svensk domstols behörighet att döma över brott som har begåtts utanför Sverige. Paragrafen innehåller sex punkter, som i huvudsak baseras på de olika folkrättsliga anknytningsprinciperna (prop. 2020/21:204 s. 146). Den omfattar bl.a. de fallen att brott har begåtts ombord på ett svenskt fartyg, av en svensk gärningsman, att brott riktats mot svenskt enskilt eller allmänt intresse och att brott har begåtts av någon som befinner sig i Sverige.

Enligt 2 kap. 12 § brottsbalken ska de begränsningar av svensk domstols behörighet och tillämpligheten av svensk lag som följer av allmän folkrätt eller av en internationell överenskommelse som är bindande för Sverige iakttas.

När det gäller frågan hur brott begångna på internet ska lokaliseras anfördes följande i förarbetena (prop. 2020/21:204 s. 99).

> Några särskilda bestämmelser om lokalisering av brott begångna på internet finns inte, utan de allmänna bestämmelserna i 2 kap. brottsbalken får tillämpas. Vid Sveriges genomförande av Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (it-brottsdirektivet), konstaterade regeringen att direktivets krav på behörighet (domsrätt) motsvarar svenska bestämmelser på området och att svenska regler om domsrätt är tillräckliga för att leva upp till direktivets krav på domsrätt för bl.a. brott som riktat sig mot ett informationssystem på medlemsstatens territorium, oavsett om gärningsmannen är fysiskt närvarande på detta territorium när brottet begås eller inte (se prop. 2013/14:92 Skärpt straff för dataintrång s. 11–13 samt jfr även SOU 2013:39 s. 245–246). Avgörande är således var en viss handling har vidtagits och var effekten har inträtt. En handling har vanligtvis begåtts vid den dator som använts för att få ett datorsystem att utföra en viss aktuell funktion, medan effekten ytterst får lokaliseras med hänsyn till den enskilda straffbestämmelsens utformning.

Vidare anfördes att det kan diskuteras om brottsbalkens generella bestämmelser är särskilt väl anpassade såvitt avser domsrätt för brottslighet med it-anknytning, men att frågan i den utsträckning det behövs får utredas i annat sammanhang (prop. 2020/21:204 s. 99 f.).

13.4 Uttalanden av intresse om behörighet att ingripa

13.4.1 Doktrinen

I doktrinen har också konstaterats att, särskilt när det gäller brott som begås med hjälp av internet, det uppstår svårigheter med frågor som rör den straffrättsliga jurisdiktionen. Det gäller också frågan om var ett sådant brott ska anses vara begånget (Agneta Bäcklund m.fl., a.a., kommentaren till 2 kap. 1 §).

Vidare har det i doktrinen anförts att ett problem med sådan brottslighet är att brotten med tillämpning av normala lokaliseringsprinciper mycket ofta kan anses begångna i Sverige. Det innebär i och för sig att Sverige mycket ofta kommer att ha jurisdiktion enligt 2 kap. 1 § brottsbalken när sådan framstår som angelägen. Det innebär emellertid också att jurisdiktionen i huvudsak är obegränsad och utan sådana ventiler (i form av bl.a. krav på åtalsförordnande) som annars gäller vid brott förövade utomlands. Om brottet har en relativt svag koppling till Sverige torde det kunna uppstå situationer där det kan upplevas som problematiskt, i vart fall om den processuella legalitetsprincipen tas på allvar (Petter Asp, Brottsbalk (1962:700), Lexino, 2024-01-01 (JUNO), kommentaren till 2 kap. 1 §).

13.4.2 Regeringens aktuella ståndpunkt

I regeringens positionspapper om tillämpningen av folkrätt i cybermiljö från juli 2022 presenterar Sverige sin allmänna ståndpunkt inom några av de områden som är centrala för en säker och trygg cybermiljö. Sverige har hittills inte sett något behov av nya regler som reglerar cyberaktiviteter, men konstaterar att cyberteknologin kan ge upphov till specifika frågor som kräver ytterligare förtydligande. Sveriges ståndpunkter är enligt ståndpunktspapperet i huvudsak följande.

Principen om staters suveräna jämlikhet gäller också i cybermiljö. Stater har likaså en skyldighet att respektera andra staters suveränitet. En överträdelse av den skyldigheten skulle utgöra en folkrättsstridig handling och ge upphov till statsansvar. En stats jurisdiktion och befogenhet gäller för personer och objekt inom dess territoriella gränser, inklusive cyberrelaterade aktiviteter. En stat har rätt att skydda personer och objekt inom sitt territorium, eller på annat sätt

under dess jurisdiktion, mot inblandning av cyberrelaterad verksamhet. En stats befogenhet och jurisdiktion inkluderar ansvar att inte medvetet tillåta att dess territorium används för handlingar som strider mot andra staters rättigheter. Generellt anser Sverige att cyberoperationer som leder till skador eller funktionsförlust kan utgöra en överträdelse av suveränitetsprincipen. Att ändra och störa data utan att orsaka fysisk skada kan också kränka en stats suveränitet (en uppfattning som uttrycks i regel 4 i Tallinnmanualen 2.0). Sådana handlingar inkluderar de som riktar sig mot cyberinfrastruktur som tillhör privatpersoner eller enheter. Inblandning i en stats inneboende statliga funktioner kan utgöra en överträdelse av statens suveränitet, även när det görs med cyberverktyg. Det måste bedömas från fall till fall, med hänsyn till intrångets natur och karaktär, om ett intrång faktiskt har lett till en överträdelse av suveräniteten.

Principen om icke-inblandning/intervention är en grundläggande regel i folkrätten som även gäller i cybermiljö. Den kan förklaras som att ingen stat eller grupp av stater har rätt att ingripa, direkt eller indirekt, av någon anledning överhuvudtaget, i någon annan stats inre eller yttre angelägenheter. Förbud mot ingripande förstås i allmänhet som två element: ingripande i frågor där varje stat får bestämma fritt och användning av tvång. Användning av tvång har ansetts särskilt uppenbar vid användning av våld, antingen i direkt form av militär aktion, eller i indirekt form av stöd till subversiva eller terroristiska väpnade aktiviteter inom en annan stat. Förbudet mot ingripande gäller mellan stater och är inte direkt tillämplig på icke-statliga aktörer. Även om de flesta cyberoperationer inte skulle innefatta användning av våld, skulle sådana operationer betraktas som sådana om de är jämförbara med omfattningen och effekterna av våldsanvändning. En bedömning måste göras från fall till fall. Enligt artikel 51 i FN-stadgan har stater rätt till självförsvar i händelse väpnat angrepp. Det är inte ett krav enligt rätten till självförsvar att det väpnade angreppet använder kinetiska medel och användningen av våld i självförsvar är inte begränsad till sådana medel.

Som en följd av deras suveränitet har stater en skyldighet att inte medvetet tillåta att deras territorium används för handlingar som strider mot andra staters rättigheter. Den väletablerade principen om due diligence[1] inom folkrätten gäller även cyberoperationer. Stater måste använda alla rimliga medel för att förhindra att deras territo-

[1] Med due diligence brukar avses en systematisk och noggrann granskning av något.

rium används för handlingar som orsakar allvarliga negativa konsekvenser för andra stater. De svårigheter som är förknippade med att upptäcka cyberaktiviteter av icke-statliga aktörer kan påverka vad en stat vet eller borde ha vetat om sådana aktiviteter. Med hänsyn till dessa svårigheter anser Sverige att den skyldigheten i princip omfattar situationer där en stat borde ha känt till skadliga aktiviteter från dess territorium.

En folkrättsstridig handling medför enligt folkrätten statsansvar även i cyberkontext.

13.4.3 Tallinnmanualen

Bakgrund

Tallinnmanualen är ett icke-rättsligt bindande vetenskapligt verk av framstående akademiker och praktiker inom folkrätten som avser att objektivt återge folkrätten som den tillämpas i cyberkontext. Manualen initierades av Natos Cooperative Cyber Defence Centre of Excellence, (CCDCOE). Den är policy- och politikneutral och representerar inte någon stats eller någon internationell organisations rättsliga ståndpunkt eller doktrin, inte heller CCDCOE:s.

Den första upplagan (år 2013) identifierar den folkrätt som är tillämplig på cyberkrigföring och anger nittiofem ”svarta bokstavsregler” som reglerar sådan krigföring. Den behandlar ämnen som suveränitet, statsansvar, jus ad bellum, internationell humanitär rätt och neutralitetsrätt. En omfattande kommentar finns till varje regel, som anger regelns grund i fördrag och sedvanerätt, förklarar hur expertgruppen tolkar tillämpliga normer i cyberkontext och beskriver eventuella oenigheter inom gruppen om varje regels tillämpning.

Den andra upplagan (The Tallinnmanual 2.0 on the international law applicable to cyber operations, 2017)[2] bygger vidare på det tidigare arbetet genom att beakta de folkrättsliga regler som tillämpas på cyberincidenter som stater stöter på dagligen, men som faller under tröskelvärdena för våldsanvändning eller väpnad konflikt, dvs. rättsliga system i fredstid. Projektet är resultatet av ett uppföljningsprojekt av en annan grupp med tjugo välrenommerade experter på folkrätt och behandlar ämnen som suveränitet, statsansvar, mänskliga rättigheter samt luft-, rymd- och havsrätt. Tallinnmanualen 2.0

[2] En tredje upplaga håller enligt uppgift på att utarbetas.

identifierar 154 ”svarta bokstavsregler” som styr cyberoperationer och innehåller omfattande kommentarer om varje regel.

Bestämmelser i Tallinnmanualen av särskilt intresse

Enligt regel 1 ”Suveränitet” gäller principen om statlig suveränitet i cybermiljön. Stater åtnjuter suveränitet över all cyberinfrastruktur som finns på deras territorium och över aktiviteter som är förknippade med den cyberinfrastrukturen.

Även om territorialitet är kärnan i suveränitetsprincipen, kan stater under vissa omständigheter utöva suveräna befogenheter, bl.a. jurisdiktion, också över cyberinfrastruktur och aktiviteter utomlands, såväl som över vissa personer som är engagerade i dessa aktiviteter (regel 10 och 11). Suveränitetens territoriella karaktär sätter också begränsningar för andra staters cyberoperationer riktade mot cyberinfrastruktur som finns på suveränt territorium (regel 4, s. 11). Av regel 2 ”Intern suveränitet” följer att en stat har suverän auktoritet – är fri att vidta alla åtgärder som den anser nödvändiga eller lämpliga – över cyberinfrastruktur, personer och cyberaktiviteter som finns på statens territorium, med förbehåll för folkrättsliga skyldigheter (s. 13).

Av regel 4 ”Överträdelse av suveränitet” framgår att en stat inte får utföra cyberoperationer som kränker en annan stats suveränitet. Regeln innebär att cyberoperationer som förhindrar eller kränker en annan stats utövande av sina suveräna befogenheter utgör en överträdelse av sådan suveränitet och är förbjudna enligt folkrätten. Det finns emellertid undantag från skyldigheten att respektera en annan stats suveränitet, t.ex. när en handling utövas i enlighet med rätten till självförsvar mot ett väpnat angrepp (regel 71). Det är endast stater som har skyldighet att respektera andra staters suveränitet enligt folkrätten och därför kan endast stater bryta mot den skyldigheten (s. 17). Ett företag som varit måltavla för en skadlig cyberoperation av en stat, kränker inte den statens suveränitet om företaget gör sig skyldig till dataintrång för att svara på den skadliga cyberoperationen. På samma sätt utgör inte cyberoperationer som utförs av en terroristgrupp, vars agerande inte kan tillskrivas en stat, en kränkning av suveräniteten av den stat som är måltavla. Det innebär dock inte att handlingarna är lagliga, tvärtom är det sannolikt att sådana

operationer bryter mot nationell lag i stater som har jurisdiktion över bl.a. de personer eller verksamheter som är inblandade. Det hindrar inte nödvändigtvis den stat som är måltavla för en cyberoperation att reagera på den i enlighet med folkrätten, t.ex. i enlighet med regeln om nödvändighet (regel 26) eller i självförsvar mot väpnade angrepp (regel 71). Suveränitetsprincipen omfattar cyberinfrastruktur som är belägen på en stats territorium oavsett om det är statlig eller privat cyberinfrastruktur (s. 18).

Enligt regel 8 ”Jurisdiktion” får en stat, med reservation för begränsningar i folkrätten, utöva territoriell och extraterritoriell jurisdiktion över cyberaktiviteter (s. 59). Territoriell jurisdiktion innebär, enligt regel 9 (s. 55), att en stat får utöva territoriell jurisdiktion över

a) cyberinfrastruktur och personer som utför cyberverksamhet på dess territorium;

b) cyberverksamhet som har sitt ursprung i eller fullbordas på dess territorium; eller

c) cyberverksamhet som har en väsentlig effekt på dess territorium.

Regel 11 avser ”Extraterritoriell verkställighetsjurisdiktion”. Den innebär att en stat endast får utöva extraterritoriell verkställighetsjurisdiktion i förhållande till personer, föremål och cyberverksamhet på grundval av en specifik befogenhetstilldelning enligt folkrätten eller giltigt samtycke från en utländsk regering att utöva jurisdiktion på dess territorium. Mot bakgrund av suveränitetsprincipen (regel 1) är verkställighetsjurisdiktion över cyberinfrastruktur, cyberverksamhet och personer som bedriver cyberverksamhet i allmänhet begränsad till den stats territorium som utövar jurisdiktionen och till fartyg och luftfartyg registrerade i den staten. Följaktligen utgör utövandet av verkställighetsjurisdiktion på en annan stats territorium en överträdelse av den statens suveränitet (regel 4) förutom i de särskilda fall som regleras i regel 11 (s. 67).

Ibland kan det vara omöjligt eller svårt att tillförlitligt identifiera den stat där digitala bevis eller andra uppgifter som är föremål för extraterritoriell verkställighetsjurisdiktion finns. Experterna är överens om att folkrätten inte tydligt behandlar den situationen. Ingen enighet kunde därför uppnås bland experterna om huruvida en stat

kan utöva extraterritoriell verkställighetsjurisdiktion i en sådan situation (s. 68).

När det gäller tillgång till elektroniska uppgifter som är allmänt tillgängliga, t.ex. på internet, utövas territoriell verkställighetsjurisdiktion, inte extraterritoriell jurisdiktion, baserat på det faktum att uppgifterna är allmänt tillgängliga i den verkställande staten (s. 69).

När det vidare gäller uppgifter som kan nås via internet men som inte är allmänt tillgängliga – exempelvis innehållet i stängda onlineforum, chattkanaler eller privata internetvärdtjänster som inte är indexerade i offentliga sökmotorer eller är dolda på Darknet – är slutsatsen densamma, så länge uppgifterna är avsedda att vara tillgängliga från den verkställande staten. Det gäller även om de är lösenordsskyddade eller på annat sätt skyddade. Om t.ex. en statlig brottsbekämpande myndighet, under falska förevändningar, kan erhålla inloggningsuppgifterna till ett slutet onlineforum som finns på servrar utomlands, men som är avsett att vara tillgängligt för en eller flera användare från staten, utövar staten territoriell verkställighetsjurisdiktion när den ansluter sig till forumet från sitt eget territorium. Sådana fall måste skiljas från de fall där uppgifter inte är avsedda att göras tillgängliga för individer i staten, t.ex. uppgifter som lagras på en privat dator utomlands, även om den är ansluten till internet, men som inte är avsedda att vara tillgängliga. Om en brottsbekämpande myndighet exempelvis gör intrång i en brottsmisstänkt persons dator som finns i en annan stat, utövar den jurisdiktion i den staten och aktiviteten kräver den senare statens samtycke eller en specifik tilldelning av befogenheter enligt internationell rätt (s. 69 f.).

Enligt regel 20 ”Motåtgärder” så kan en stat under vissa förutsättningar ha rätt att vidta motåtgärder, oavsett om de är av cyberkaraktär eller inte, som svar på en folkrättsstridig handling som en annan stat har vidtagit. I regel 21–26 finns bestämmelser som närmare reglerar den situationen.

13.4.4 Svensk och utländsk rättspraxis

Det finns bara ett fåtal rättsfall som kan bidra till att belysa jurisdiktionsfrågan. De avser emellertid domsrätt snarare än verkställighetsjurisdiktion.

Norges Høyesterett prövade i ett avgörande den 28 mars 2019 (HR 2019–619-A i sak nr 19-010640STR-HRET) frågan om det var tillåtet för polisen att från dataterminaler i ett företags lokaler i Oslo ladda ner elektroniskt material som företaget själv hade lagrat på en utländsk server eller om sådan tvångsmedelsanvändning faller utanför norska myndigheters jurisdiktion.

Norges Høyesterett fann, med hänvisning till andra anknytningsfaktorer än lagringsplatsen, att det fanns norsk jurisdiktion för åtgärden (p. 67–69). Vidare konstaterade domstolen att materialet behålls på den utländska servern, att inga ändringar görs i det lagrade materialet, exempelvis i form av radering eller blockering och att eventuella beslag görs tillgängliga i egna lagringsenheter i Norge (p. 70). Domstolen fann att, genom att materialet kopieras vid polisens genomsökning, åtgärden inte påverkar en annan stat på ett sådant sätt att det utgör en kränkning av suveränitetsprincipen (p. 71).

En liknande fråga kom senare att prövas av Högsta domstolen. Rättsfallet NJA 2023 s. 231 ”Den okända lagringsplatsen” avsåg användning av genomsökning på distans enligt 28 kap. 10 a–10 i §§ RB. Det tvångsmedlet gör det möjligt att i en förundersökning få tillgång till elektroniska uppgifter som kan ha betydelse som bevis och som finns lagrade på t.ex. externa servrar eller i s.k. molnbaserade internettjänster.

Prejudikatfrågan var om genomsökning på distans får beslutas även när den information som genomsökningen avser kan vara lagrad i utlandet. Högsta domstolen konstaterade att RB:s bestämmelser om genomsökning på distans är utformade så att de medger eftersökning av information som finns lagrad utanför Sverige (p. 17–20).

Vidare konstaterade Högsta domstolen (p. 22) att det följer av 2 kap. 12 § brottsbalken, eller grunderna för den, att en stats verkställande jurisdiktion är begränsad till den statens territorium och att staten alltså är förbjuden att vidta verkställighetsåtgärder på andra staters territorium. Det är fråga om tillämpning av den folkrättsliga s.k. territorialitetsprincipen när det gäller verkställighetsåtgärder. Det finns enligt Högsta domstolen inte några folkrättsliga hinder mot att myndigheter bereder sig tillgång till elektronisk information som är eller kan vara lagrad i servrar utanför den egna statens territorium (p. 22–39). En genomsökning på distans kan enligt Högsta domstolen göras under förutsättning att åtgärden vidtas inom ramen för en svensk brottsutredning och är föranledd av en misstanke om

brott som faller inom svensk dömande jurisdiktion. Det måste förutsättas att åtgärden vidtas med användning av utrustning som finns i Sverige och att den görs på ett sådant sätt att den eftersökta informationen inte raderas eller på annat sätt påverkas till sitt innehåll (p. 40). Högsta domstolen ansåg att det inte fanns anledning att därutöver ställa upp några särskilda krav på anknytning till Sverige.

Frågan utreddes samtidigt av 2021 års datalagringsutredning, som bl.a. hade i uppdrag att analysera och utvärdera regleringen om lagring av och tillgång till uppgifter om elektronisk kommunikation för brottsbekämpande syften i förhållande till ny praxis från EU-domstolen. Uppdraget var även att se över vissa frågor om svenska myndigheters tillgång till elektroniska uppgifter, när de finns utanför Sveriges gränser (exekutiv jurisdiktion). Utredningen redovisade sina slutsatser i betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22 s. 431 f.). Utredningens förslag ligger i linje med Högsta domstolens avgörande i NJA 2023 s. 231. Betänkandet bereds i Regeringskansliet.

Högsta domstolen prövade vidare i rättsfallet ”Internetförtalet” frågan om svensk domstol är behörig att pröva ett åtal för förtal som begåtts via internet, när åtgärderna för att publicera uppgifterna har vidtagits utanför Sverige (p. 9).

Högsta domstolen konstaterade inledningsvis att det inte finns några särskilda bestämmelser om lokalisering av brott som begåtts på internet, utan att de allmänna bestämmelserna i 2 kap. brottsbalken får tillämpas. Avgörande är således var en viss handling har vidtagits och var effekten har inträtt. En handling har vanligtvis vidtagits vid den dator eller motsvarande som använts för att få ett datasystem att utföra en viss aktuell funktion, medan effekten ytterst får lokaliseras med hänsyn till hur den enskilda straffbestämmelsen är utformad (p. 15).

Vidare konstaterade Högsta domstolen att, när en förtalsgrundande uppgift publiceras på internet från utlandet, blir det som avgör om det föreligger svensk domsrätt enligt 2 kap. 1 § brottsbalken, om effekten av förtalsbrottet kan anses ha inträtt i Sverige (p. 16). Ett förtalsbrott som begås genom att uppgifter publiceras på internet fullbordas enligt Högsta domstolen när tredje man får kännedom om uppgifterna. Då uppstår också risken att den som uppgifterna rör utsätts för andras missaktning. Det ligger nära till hands att hävda att effekten, i den mening som avses i 2 kap. 1 § andra stycket,

inträder vid den tidpunkten (p. 17). Följden av ett sådant synsätt är dock enligt Högsta domstolen att effekten kan lokaliseras till samtliga platser där uppgifterna kommit till tredje mans kännedom. Svensk domstols behörighet att döma över förtal begånget på internet skulle därmed vara i princip obegränsad (p. 18).

Att de förtalsgrundande uppgifterna kommit till tredje mans kännedom kan därför inte enligt Högsta domstolen anses tillräckligt för att effekten av brottet, i den mening som avses i 2 kap. 1 § andra stycket, ska anses ha inträtt i Sverige. En förutsättning bör därutöver vara att det finns en relevant koppling till Sverige. Bedömningen av om det finns en sådan koppling bör grundas på objektivt konstaterbara omständigheter som exempelvis att uppgifterna avser svenska medborgare eller andra som är bosatta här. En annan omständighet som kan beaktas är om uppgifterna är avsedda huvudsakligen för svenska mottagare. Så kan vara fallet om uppgifterna har lagts ut på en svensk hemsida eller någon annan digital plattform som riktar sig främst till en svensk publik. Bedömningen av kopplingen till Sverige måste göras med beaktande av samtliga omständigheter i det enskilda fallet (p. 19). Om det finns en relevant koppling till Sverige hindrar, enligt Högsta domstolen, inte det förhållandet att uppgifterna i det enskilda fallet först nåtts av en tredje man i utlandet att effekten även bedöms ha inträtt här (p. 21).

13.5 Lagens tillämpningsområde bör begränsas

13.5.1 Den nya lagen ska vara förenlig med folkrätten

Utredningens bedömning

Den nya lagens tillämpningsområde behöver begränsas för att vara förenlig med folkrätten.

Skälen för utredningens bedömning

Ett grundläggande problem när det gäller diskussionen om ingripanden i cybermiljö är den stora skillnaden mellan ingripanden i fysisk miljö och ingripanden i cybermiljö och att den rättsliga reglering som finns utgår från den fysiska miljön. I en fysisk miljö är det lätt

att iaktta och beakta gränser, medan en virtuell miljö inte har samma gränser. Det är genom den moderna tekniken som skillnaderna mellan fysisk och virtuell miljö har kommit att ställas på sin spets, eftersom tekniken i dag möjliggör att åtgärder kan vidtas på distans.

Vid utformningen av den nya lagens tillämpningsområde ska hänsyn tas till principen om staters suveräna jämlikhet i cybermiljön men även skyldighet att respektera andra staters suveränitet. Eftersom cybermiljön saknar traditionella gränser krävs det särskilda begränsningar av den nya lagens tillämpningsområde för att myndigheternas ingripanden inte ska strida mot folkrätten. Begränsningarna bör utgå från faktorer som tydligt anknyter till Sverige, på samma sätt som gäller för svensk domsrätt.

Det kan tilläggas att, även om Tallinnmanualen ger uttryck för ett antal framstående akademikers ståndpunkt, finns det utrymme för andra ståndpunkter om vilka åtgärder som kan vara tillåtna för en myndighet att vidta i cybermiljön. Polismyndigheten har särskilt pekat på att Nederländerna har en från Sverige avvikande ståndpunkt i den frågan.

13.5.2 Anknytningen till svenska förhållanden

Utredningens förslag

Lagen är tillämplig på brott, eller brottslig verksamhet som innefattar sådant brott, som begås eller kommer att begås i cybermiljö med hjälp av informationssystem om brottet begås av någon som befinner sig i Sverige, om brottet riktas mot någon eller något som befinner sig i Sverige eller om informationssystemet finns i Sverige.

Skälen för utredningens förslag

Utgångspunkter

Vid utformningen av tillämpningsområdet och de brottsbekämpande myndigheternas befogenheter att ingripa bör utgångspunkten vara territorialprincipen och de olika lokaliseringsbestämmelser som kommer till uttryck i 2 kap. 1 § brottsbalken.

Tillämpningsområdet för lagen kommer emellertid att begränsas även på andra sätt än de som behandlas i detta kapitel. Som har konstaterats i avsnitt 13.1.2 ska lagen vara tillämplig både på brott och brottslig verksamhet. I avsnitt 14.6 utvecklar utredningen skälen för att ingripandena endast bör få avse brott eller brottslig verksamhet som innefattar brott av viss svårhetsgrad. Vidare diskuteras behovet av en uttrycklig proportionalitetsregel i avsnitt 14.7.

Brott som begås av någon som befinner sig i Sverige

Lagen bör för det första vara tillämplig på brott som begås eller kommer att begås i cybermiljö med hjälp av informationssystem om gärningsmannen eller gärningsmännen, när brottet eller brotten begicks eller skulle begås, befann sig i Sverige. Det innebär att det ställs krav på att gärningen åtminstone ska påbörjas här i landet, men att delar av den kan utföras i ett annat land. Det som nu har sagts om gärningsmannen bör gälla även annan medverkande.

Brott som riktas mot någon eller något i Sverige

Ingripande enligt lagen bör också vara möjligt när det tänkta målet för brottet eller brotten finns i Sverige. Det bör vara effekten av brottet eller brotten eller det tänkta målet för brotten som gör lagen tillämplig. Det kan röra sig om brott som är avsedda att orsaka ekonomisk eller annan skada eller fara som kan uppstå i Sverige. Målet för brotten kan vara fysiska personer som befinner sig i Sverige, oavsett om brottet riktar sig mot en obekant krets av sådana personer eller en viss person. Målet kan även vara företag eller andra juridiska personer i Sverige, men även svenska myndigheter och kommuner eller andra motsvarande organ. Brotten behöver inte alltid involvera informationssystem i Sverige, utan det är tillräckligt att gärningsmannen begår brottet eller brotten i cybermiljö med hjälp av ett informationssystem och att brottet riktas mot någon eller något här i landet. Ett brott anses normalt sett vara riktat mot den som är att bedöma som målsägande, dvs. den mot vilken brott har begåtts eller som blivit förnärmad eller lidit skada av brottet (se 20 kap. 8 § fjärde stycket RB).

Det tänkta målet för brottet eller brotten kan även vara informationssystem som finns i Sverige, utan att det finns en koppling till något av de nyss nämnda subjekten. Det kan röra sig om dataintrång som riktas mot informationssystem i Sverige, exempelvis angrepp genom spridning av virus, skadlig kod eller liknande. Det kan också vara fråga om utpressnings- eller bedrägeriangrepp som slumpvis riktas mot svenska mål, vilket kan framgå genom att de riktar sig mot en svensk publik. Även dataintrång som riktar sig mot informationssystem i Sverige, i syfte att kunna använda dem som ett hjälpmedel för framtida brott (t.ex. i ett anonymiseringsnätverk), hör hit.

Det saknar alltså betydelse var gärningsmannen eller gärningsmännen som utför brott med hjälp med av ett informationssystem befinner sig, om brottet riktar sig mot någon eller något i Sverige.

Rätten att ingripa bör även omfatta brott som riktar sig mot den svenska staten (jfr 2 kap. 3 § 4 brottsbalken). Det kan röra sig om fall där brottet i sin helhet begås utomlands men där brottet riktar sig mot ett intresse som den svenska staten uppfattas som bärare av, bl.a. brott mot rikets säkerhet, allmän verksamhet eller annat av rättsordningen särskilt skyddat svenskt intresse. Dit hör alltså brott mot svenska statens yttre eller inre säkerhet eller mot offentliga myndigheter, vilket innebär att huvuddelen av brotten i 17–22 kap. brottsbalken omfattas. Det omfattar också t.ex. smuggling och brott mot svensk valutareglering (jfr Agneta Bäcklund m.fl., a.a., kommentaren till 2 kap. 3 §).

Anknytning till informationssystem som finns i Sverige

Något som skiljer sig mellan brott i cybermiljö och brott i fysisk miljö är att det i de förstnämnda fallen inte alltid behöver finnas någon fysisk person som ligger bakom de enskilda brotten. Den tekniska utvecklingen medger nämligen att särskilda dataprogram skapas som automatiskt utför vissa handlingar som initierar brott. Det kan exempelvis vara fråga om att automatiskt söka efter viss information eller att flytta vissa data. Det finns därför också behov av att kunna ingripa vid fall där de nyss nämnda anknytningsfaktorerna, t.ex. gärningsmannens eller något brottsoffers lokalisering i Sverige, är okända men det är känt vilket informationssystem som brottet

begås med hjälp av, under förutsättning att det informationssystemet finns i Sverige.

Det kan även vara fråga om att någon i ett annat land utnyttjar informationssystem eller servrar som finns i Sverige för ett cyberangrepp mot ett mål i ett tredje land. Det kan t.ex. vara fråga om informationssystem som finns i hallar med servrar som ägs eller används av personer eller företag i Sverige. Det kan också vara fråga om annan elektronisk utrustning som finns i Sverige som är uppkopplad mot internet, som används som hjälpmedel för att begå brott eller som utnyttjas i brottslig verksamhet. Ett typiskt exempel är noder som ingår i ett anonymiseringsnätverk där det informationssystem som angriparen använder sig av finns utomlands eller är okänt. Eftersom det är viktigt att förhindra att Sverige används som en fristad för att begå brott i cybermiljö bör därför ingripanden enligt lagen vara möjliga om det eller de informationssystem som används för ett angrepp i cybermiljö finns i Sverige.

Förhållandet mellan anknytningsfaktorerna

Anknytningsfaktorerna är alternativa. Med andra ord är det tillräckligt att en av dem är uppfylld för att den nya lagen ska bli tillämplig.

Det innebär att lagen kan tillämpas om gärningsmannen befinner sig här i landet men brottet riktas mot något eller någon utanför Sverige. Med dagens teknik bör det visserligen i praktiken vara ovanligt att en gärningsman befinner sig i Sverige samtidigt som informationssystemet som han eller hon begår, eller kommer att begå, brott med hjälp av inte också finns i Sverige. Utredningen vill dock inte utesluta den möjligheten. Ett exempel kan vara att någon i Sverige skapar en programvara som kan användas för dataintrång eller som är skräddarsydd för att användas för andra brott i cybermiljö och sedan förmår någon i ett annat land att använda programmet i brottsligt syfte. En annan sak är att ett brott kan begås med hjälp av flera informationssystem på så sätt att det informationssystem som initialt används av gärningsmannen är sammanlänkat med eller kommunicerar med andra informationssystem som finns i olika delar av världen.

Vidare innebär regleringen att lagen är tillämplig om en gärningsman inte befinner sig i Sverige och begår brott med hjälp av ett in-

formationssystem som inte heller finns sig i Sverige, men brottet riktas mot någon eller något i Sverige.

Slutligen innebär det att lagen är tillämplig även om en gärningsman inte befinner sig i Sverige och begår brott mot någon eller något som inte heller befinner sig i Sverige, men brottet begås med hjälp av ett informationssystem som finns i Sverige. Som nyss konstaterats bör det i praktiken handla om informationssystem som kommunicerar med det informationssystem som gärningsmannen initialt använder sig av och som i regel finns i nära fysisk anslutning till gärningsmannen.

Internationellt rättsligt samarbete

Som tidigare framhållits finns det olika praktiska problem som förknippas med ingripanden mot brott och brottslig verksamhet i cybermiljö. Till problemen hör att flera olika jurisdiktioner kan vara inblandade i samma brottsliga gärning, beroende på att gärningsman, brottsoffer och bevisning kan befinna sig i olika delar av världen. Det innebär att internationellt rättsligt samarbete kan komma att få en framträdande roll i enskilda fall i förhållande till stater som är villiga att samarbeta. Enligt utredningens mening skiljer sig dock inte de åtgärder som på svensk begäran kan behöva vidtas i andra länder från åtgärder av samma slag i brottsutredningar i allmänhet eller i underrättelseverksamhet, oavsett om det rör sig om ett ingripande mot en server i fysisk form eller i cybermiljö.

Det bör i detta sammanhang understrykas att möjligheten att ingripa enligt den nya lagen inte sträcker sig så långt att ett ingripande får riktas mot t.ex. en känd server eller annat informationssystem som finns i ett annat land utan att det finns någon anknytning till Sverige på det sätt och under de förutsättningar som utredningen föreslår. Det skulle vara att gå utöver det som anses ligga inom en stats exekutiva jurisdiktion.

13.6 Slutsatser om lagens tillämpningsområde

Utredningens bedömning

Den nya lagens tillämpningsområde är förenligt med rättspraxis och doktrin när det gäller frågan om jurisdiktion och står inte heller i strid med folkrätten.

Skälen för utredningens bedömning

Ett område där det saknas klara regler

Som redan framgått är cybermiljön ett komplext juridiskt område, där det inte finns någon tydlig författningsreglering. Den rättspraxis som finns är fragmentarisk. Det finns i och för sig vissa internationella överenskommelser om judiciellt samarbete, men det regelverket täcker bara vissa företeelser. Det kan således konstateras att vägledning för vilka ingripanden som kan vara godtagbara får sökas på andra ställen. Staternas positionspapper om hur folkrätten bör tillämpas i cybermiljö och Tallinnmanualen kan bidra till ökad tydlighet. Det bör dock framhållas att de har sin bakgrund i överväganden beträffade annat än traditionell brottsbekämpning.

Skäl som talar för att tillämpningsområdet utformas enligt förslaget

Inledningsvis kan konstateras att de anknytningsfaktorer som utredningen föreslår ligger i linje med artikel 9[3] i Tallinnmanualen.

Enligt regel 4 i Tallinnmanualen är huvudregeln att en stat begår en överträdelse av suveräniteten om staten utför cyberoperationer som förhindrar eller kränker en annan stats utövande av sina suveräna befogenheter. Det är endast stater som är skyldiga att respektera andra staters suveränitet enligt folkrätten och därför kan endast stater bryta mot den skyldigheten. Enligt regeringen anser Sverige att överträdelse av suveräniteten kan uppstå vid cyberoperationer som leder till skador eller funktionsförlust (se avsnitt 13.4.2). Att ändra och störa data utan att orsaka fysisk skada kan också utgöra en överträdelse av suveräniteten. Det kan hävdas att den inställningen

[3] Hänvisningarna till Tallinnmanualen avser version 2.0.

utgör hinder mot att brottsbekämpande myndigheter ”initierar” ett ingripande, eftersom det inte anses som ett svar på ett tidigare angrepp som strider mot folkrätten enligt regel 20 i Tallinnmanualen, utan endast brott enligt nationell rätt. I sådana fall skulle de brottsbekämpande myndigheternas agerande kunna utgöra en överträdelse av suveränitetsprincipen. I regel 71 i Tallinnmanualen görs undantag från regel 4 vid väpnade konflikter. Det undantaget kan inte heller generellt sägas vara tillämpligt vid brott i cybermiljö.

Brottsbekämpande myndigheters ingripande mot brott regleras emellertid särskilt i regel 11 i Tallinnmanualen, som innebär att en stat endast får utöva extraterritoriell verkställighetsjurisdiktion i förhållande till personer, föremål och cyberverksamhet på grundval av en specifik befogenhetstilldelning enligt folkrätten eller giltigt samtycke från en utländsk regering att utöva jurisdiktion på sitt territorium. Mot bakgrund av suveränitetsprincipen (regel 1) är verkställighetsjurisdiktion över cyberinfrastruktur, cyberverksamhet och personer som bedriver cyberverksamhet i allmänhet begränsad till den stats territorium som utövar jurisdiktionen och till fartyg och luftfartyg registrerade i den staten.

Samtidigt finns det inte några folkrättsliga begränsningar för svenska brottsbekämpande myndigheter att skaffa sig tillgång till information som är lagrad i utlandet eller på okänd plats (jfr p. 34 i ”Den okända lagringsplatsen”). Det är vidare tydligt att det inte heller finns någon rättspraxis som innebär att brottsbekämpande myndigheter är förhindrade att bereda sig tillgång till elektronisk information som är eller kan vara lagrad i informationssystem utanför den egna statens territorium (jfr p. 38 i ”Den okända lagringsplatsen” och s. 68 i Tallinnmanualen).

I fråga om tillgång till elektroniska uppgifter som finns på servrar utomlands och är allmänt tillgängliga, t.ex. genom internet, utövar en stat dessutom i de situationerna territoriell, i motsats till extraterritoriell, verkställighetsjurisdiktion baserad på det faktum att uppgifterna är allmänt tillgängliga i deras stat. Detsamma gäller uppgifter som inte är allmänt tillgängliga, exempelvis innehållet i stängda onlineforum, chattkanaler eller privata internetvärdtjänster som inte är indexerade i offentliga sökmotorer eller är dolda på Darknet, så länge uppgifterna är avsedda att vara tillgängliga från den berörda staten (s. 69 i Tallinnmanualen).

Utredningen kan även konstatera att det i en stats rätt till suveränitet inte bara ligger att staten får ingripa mot brott på sitt territorium utan också att staten har skyldighet att inte medvetet tillåta att territoriet används för handlingar som strider mot andra staters rättigheter (principen om due diligence). Det gäller även cyberoperationer. Stater måste använda alla rimliga medel för att förhindra att deras territorium används för handlingar som orsakar allvarliga negativa konsekvenser för andra stater. Svårigheterna att upptäcka cyberaktiviteter av icke-statliga aktörer kan påverka vad en stat vet eller borde ha vetat om sådana aktiviteter. I princip anses Sveriges skyldighet omfatta situationer där staten borde ha känt till skadliga aktiviteter som utförs på vårt territorium (se avsnitt 13.4.2). Den principen får betydelse för den nya lagens tillämplighet när det gäller brott som begås med hjälp av t.ex. informationssystem som finns i Sverige men som riktar sig mot andra stater, t.ex. informationssystem som finns i Sverige och som ingår i ett anonymiseringsnätverk.

Slutsatser

Utredningen anser att varje stats skyldighet enligt bl.a. Europakonventionen att skydda sina egna medborgare mot brottsliga angrepp hittills har fått stå tillbaka i de diskussioner som har förts om vilka åtgärder som kan vara godtagbara i cybermiljön. Det finns därför inte någon nämnvärd lagstiftning på området. Det är troligen det som utgör en del av förklaringen till att brott och brottslighet i den miljön har vuxit så kraftigt på senare tid. Mot den bakgrunden skulle en reglering som i stor utsträckning bygger på hjälp från andra länders judiciella myndigheter inte ge svenska brottsbekämpande myndigheterna de verktyg som efterfrågas.

I den australienska lagstiftningen (se avsnitt 10.3) ställs det krav på samtycke av den stat i vilken det informationssystem finns, eller uppgifterna i systemet, som ingripandet riktar sig mot innan några åtgärder får vidtas. Ett motsvarande krav skulle enligt utredningens mening i alltför hög grad begränsa möjligheterna att tillämpa den nya lagen, särskilt mot bakgrund av hur snabbt uppgifter i digitala miljöer kan flyttas från ett land till ett annat.

Den lag som utredningen föreslår ger brottsbekämpande myndigheter befogenhet att, med användning av teknisk utrustning som finns i Sverige, ingripa mot brott och brottslig verksamhet i cybermiljö. Ingripandena ska föranledas av att brott begås eller brottslig verksamhet bedrivs med hjälp av informationssystem, som ska ha tydlig anknytning till Sverige. Genom förslagen i den nya lagen ges de brottsbekämpande myndigheterna möjlighet att ingripa på ett sådant sätt att uppgifter får påverkas till sitt innehåll eller raderas. Om syftet med ingripandet är att radera uppgifter ställs det särskilda krav (se avsnitt 14.5.2). Den anknytning till Sverige som föreslås ligger enligt utredningens mening väl i linje med befintlig reglering och doktrin. Enligt utredningens mening är förslaget, genom den anknytning till svenska förhållanden som är en förutsättning för att lagen ska vara tillämplig, förenlig med Sveriges internationella åtaganden.

14 Olika former av ingripanden

14.1 Ändamålen med ingripandena

14.1.1 Ändamålsprincipen

Som framgått av avsnitt 12.3.1 ger regleringen i 8 § polislagen och 2 kap. 2 § tullbefogenhetslagen uttryck för bl.a. ändamålsprincipen när en tjänsteuppgift ska verkställas. För att säkerställa att ingripanden i cybermiljö verkställs på ett rättssäkert sätt bör en grundläggande utgångspunkt vara att ändamålen med ingripandena kommer till direkt uttryck i den nya lagen. På så sätt begränsas också tillämpningsområdet. Ett ingripande bör endast få göras för de ändamål som anges i den nya lagen. Innan en åtgärd beslutas för ett visst ändamål ska beslutsfattaren alltid pröva om åtgärden förväntas uppfylla ändamålet. Om så inte är fallet får åtgärden inte användas.

Med hänsyn till att det övergripande syftet med den nya regleringen är att de brottsbekämpande myndigheterna ska ha befogenheter att ingripa mot brott och brottslig verksamhet i cybermiljö, är det en naturlig utgångspunkt vid utformningen av ändamålen.

14.1.2 Närmare om ändamålen

Utredningens förslag

Om det är av särskild vikt för att förhindra eller avbryta brott eller störa eller avbryta brottslig verksamhet i cybermiljö får Polismyndigheten, Säkerhetspolisen eller Tullverket ingripa på visst sätt som specificeras i lagen.

Detsamma gäller om det kan antas att ett informationssystem utnyttjas i brottslig verksamhet i cybermiljö och det är av särskild vikt att kunna kartlägga om det i den brottsliga verksamheten förekommer kommunikation med andra informationssystem.

Skälen för utredningens förslag

Flera ändamål som kompletterar varandra

Vid den tidpunkt när en brottsbekämpande myndighet får kännedom om något som tyder på att det förekommer brott, eller i vart fall brottslig verksamhet, i cybermiljö är de närmare omständigheterna kring gärningen normalt inte kända. Det är således oklart om det handlande som myndigheterna ser skäl att ingripa mot konstituerar ett fullbordat brott, utgör en osjälvständig brottsform eller ännu inte har nått till den nivån att handlandet är straffbart. För att få en så heltäckande lagstiftning som möjligt bör därför ändamålen med ingripandena komplettera varandra och motsvara alla tänkbara stadier av brottsliga förehavanden i cybermiljö.

Förhindra brott i cybermiljö

Som nyss nämnts bör ingripanden i cybermiljö omfatta bl.a. möjlighet att ingripa för att förhindra brott i cybermiljö innan de begås. Det innebär att handlingen som konstituerar brottet inte ska ha kommit så långt att den i det enskilda fallet kan bedömas som stämpling, förberedelse eller försök till brott. Det bör vara tillräckligt att underrättelseinformation eller andra omständigheter ger ett objektivt underlag för bedömningen att ett visst brott planeras eller ska påbörjas. Det räcker däremot inte med allmänna antaganden eller

med spekulationer om att så är fallet, utan det krävs någon faktisk omständighet som ger stöd för det. Det kan t.ex. vara fråga om en långt framskriden brottsplan. Sådana kan numera köpas genom det som kallas crime as a service.

Huvudsyftet med den nya lagen är att så långt möjligt förhindra brott i cybermiljö. Det innebär att ingripanden kan leda till att något brott inte hinner begås. Beroende på omständigheterna i varje enskilt fall kan behovet av att förhindra brott ibland vara större än behovet av att utreda gärningen. Det kan handla om att ingripa mot någon som är involverad i en pågående brottsserie, t.ex. ett antal bedrägerier som med hjälp av digital teknik, på ett likartat sätt och under samma tidsperiod riktas mot flera personer. Ett annat exempel kan vara att genom ett ingripande hindra slumpvis utsända meddelanden som lockar mottagarna att klicka på länkar med skadlig programvara eller som förmår dem att avslöja inloggningsuppgifter som kan användas för brott. Det kan också handla om försäljning av narkotika genom en marknadsplats på internet, där framtida köp av narkotika förhindras genom ett ingripande mot marknadsplatsen. Oavsett om ett visst brott har hunnit fullbordas kan det ibland vara av större värde att ingripa och förhindra att nya brott begås mot andra personer, än att få underlag för att utreda och lagföra de begångna brotten.

Det kan uppkomma situationer där den brottsbekämpande myndigheten misstänker att ett brott i cybermiljö kommer att begås, som i sin tur är ett led i att brott i fysisk miljö senare kommer att begås. Ett typiskt exempel är situationer där crime as a service används för att locka unga att begå allvarliga brott, t.ex. våldsbrott, vilket numera kan vara straffbart som involverande av en underårig i brottslighet. Om ett ingripande äger rum i ett så tidigt skede att cyberbrottet kan förhindras kommer det även att innebära att brott i fysisk miljö förhindras. Ett annat exempel kan vara ett ransomwareangrepp, som kan leda till att utpressningspengar betalas ut, men om angreppet kan förhindras finns det inga förutsättningar för utpressning. Syftet med den nya regleringen är inte att ingripanden i cybermiljö ska förhindra att brott i fysisk miljö begås. Det kan däremot bli en positiv bieffekt t.ex. om en marknadsplats för att sälja illegala varor blockeras eller stängs ner.

Rättssäkerhetsskäl och den ingripande karaktären som ingripanden i cybermiljö kan ha, talar enligt utredningen för att ett särskilt ändamål för ingripande bör vara att förhindra konkreta brott. Syftet

med ett ingripande får alltså inte enbart vara att förhindra en till sitt innehåll ospecificerad brottslig verksamhet. Däremot är det viktigt att kunna störa eller avbryta brottslig verksamhet i cybermiljö, vilket i enskilda fall även kommer att leda till att konkreta brott förhindras. Det senare bör dock, som utredningen återkommer till, vara ett särskilt ändamål.

Sammanfattningsvis anser utredningen att ett ändamål med ingripanden enligt den nya lagen ska vara att förhindra att brott i cybermiljö begås.

Avbryta brott i cybermiljö

Ingripanden i cybermiljö bör även kunna omfatta situationer där det finns förutsättningar att inleda förundersökning om konkreta brott. Det kan, på samma sätt som i den fysiska miljön, uppstå fall där det inte är möjligt att förhindra att ett brott begås i cybermiljö, om brottet upptäcks först sedan det har påbörjats. Det handlar alltså om att ingripandet äger rum på ett stadium när brottet är att bedöma som stämpling, förberedelse eller försök till brott men där brottet ännu inte har hunnit fullbordas. Mot bakgrund av att viss brottslighet är systematisk och bedrivs mer eller mindre kontinuerligt, t.ex. narkotikaförsäljning på Darknet, kan det förutses att det vid ett planerat ingripande förekommer brottsligt handlande i olika stadier av fullbordan. Ett ingripande bör, beroende på vilken underrättelseinformation som finns och hur tillförlitlig den är, kunna göras både i ett relativt tidigt skede, så snart det är fråga om en handling som kan utgöra straffbar planering eller förberedelse, och vid ett nära förestående konkret brott.

I många fall kan det dock vara svårt att avgöra hur långt brottsplaner har hunnit förverkligas. Ett exempel kan vara att det upptäcks att en person på ett forum på internet erbjuder sig att tillverka skjutvapen på beställning eller att tillhandahålla någon annan kriminaliserad tjänst. Det saknas då kunskap om personen i fråga redan har gjort sig skyldig till ett fullbordat brott eller ett osjälvständigt brott eller bara planerar framtida brottslig verksamhet, men det är samtidigt viktigt att polisen kan avbryta agerandet så snart som möjligt. Ett annat exempel kan vara ett ingripande mot vad som tros vara ett enstaka brott men som visar sig vara en del av en seriebrottslighet.

Det kan även vara fråga om systematiska bedrägerier, där det är okänt om något brott har fullbordats men det är sannolikt att det bara är en tidsfråga innan det sker.

Ingripandet ska syfta till att brottet eller brotten inte ska fullbordas. Det kan dock inte uteslutas att vissa omständigheter även uppfyller rekvisiten för ett annat, mindre allvarligt, brott som eventuellt hinner fullbordas. Ett ingripande för att avbryta brott i cybermiljö kan också, på samma sätt som ingripanden i den fysiska miljön, ge underlag för att utreda redan fullbordade brott av samma eller annat slag (se avsnitt 20.1 om förhållandet till andra brottsbekämpande åtgärder).

Även om syftet med ett ingripande är att brott i cybermiljö ska avbrytas, kan resultatet av ingripandet i ett enskilt fall bli att gärningsmannen endast störs och att brottet alltså inte avbryts. Det hindrar inte att ingripandet kan ha varit välgrundat.

Sammanfattningsvis anser utredningen att ett ändamål med ingripanden enligt den nya lagen ska vara att avbryta brott i cybermiljö.

Störa eller avbryta brottslig verksamhet i cybermiljö

Som nyss nämnts bör ingripanden i cybermiljö omfatta bl.a. möjlighet att ingripa för att störa eller avbryta brottslig verksamhet. Den brottsliga verksamheten ska helt eller delvis bedrivas i cybermiljö. Som framgått bedrivs det en omfattande verksamhet i cybermiljö vars enda, eller huvudsakliga, ändamål är brottsliga. Det är då viktigt att myndigheterna kan störa den brottsliga verksamheten. Det kan uppstå situationer på underrättelsestadiet där den brottsliga verksamheten är känd, men där det inte är möjligt att förhindra att konkreta brott kommer att begås. Skälet till det kan vara att alla omständigheter kring brottet eller brotten inte är kända för myndigheten, utan endast att vissa omständigheter i den tillgängliga underrättelseinformationen tyder på att det rör sig om en viss form av brottslig verksamhet (som innefattar en eller flera kriminaliserade gärningar), exempelvis bedrägeribrottslighet.

Som tidigare nämnts kan det, när ett ingripande aktualiseras, vara svårt – och ibland omöjligt – att avgöra om det är fråga om pågående enskilda brott, en brottslig verksamhet som är systematisk eller ett visst handlande som kan utmynna i ett eller flera nära förestående

brott. För att göra den nya lagstiftningen så heltäckande som möjligt bör möjligheten att ingripa därför även omfatta att störa eller avbryta brottslig verksamhet.

Om det pågår brottslig verksamhet är det angeläget att vidta åtgärder för att försvåra att svenska intressen utsätts för brott. Ett typiskt exempel kan vara bedrägerier, där det finns underrättelseinformation, t.ex. annonser på internet, som tyder på att det förekommer investeringsbedrägerier, men där varken de som ligger bakom brotten, de enskilda brotten, målsägandena eller andra fakta som behövs för att urskilja ett konkret brott är kända. Ett annat exempel kan vara att någon varnas för en kommande ransomwareangrepp och kan lämna tillräcklig information för att ett ingripande ska kunna riktas mot ett visst informationssystem. Ett ytterligare exempel kan vara när myndigheten tidigt får kännedom om att någon håller på att skapa ett bot-nät, men det ännu inte har aktiverats eller har erbjudits som crime as a service.

Att störa eller avbryta brottslig verksamhet kan bestå i olika åtgärder som försvårar den pågående verksamheten. Det kan t.ex. vara fråga om att blockera tillgången till en viss hemsida som uppmuntrar till brott eller att begränsa tillgången till uppgifter som ger möjlighet att komma åt uppgifter som, om de överförs, leder till ett fullbordat brott. Olika åtgärder för att begränsa tillgång till övergreppsmaterial eller innehåll som uppmuntrar till terroristbrott är andra exempel. Ingripanden kan också bestå i att hindra spridning av vissa uppgifter som inte har någon legal användning men som kan utnyttjas för framtida brott, t.ex. listor med läckta personuppgifter, lösenordsuppgifter eller kontokortsuppgifter.

Effekten av ett ingripande enligt den nya lagen kan, som tidigare nämnts, indirekt bli att brott förhindras eller att brottslig verksamhet störs eller avbryts även i den fysiska miljön. Ett exempel kan vara att en webbplats, som rekryterar personer som är villiga att begå fysiska brott mot betalning eller som används för att erbjuda olagliga sexuella tjänster, stängs ner.

Sammanfattningsvis anser utredningen att ett ändamål med ingripanden enligt den nya lagen bör vara att störa eller avbryta brottslig verksamhet i cybermiljö.

Kartlägga kommunikation mellan informationssystem som utnyttjas i brott eller brottslig verksamhet

Säkerhetspolisen har särskilt lyft behovet av att kunna vidta åtgärder för att kartlägga om ett informationssystem, t.ex. en nätverksansluten enhet, eller ett användarkonto eller en på annat sätt avgränsad del av ett informationssystem, utnyttjas i brott eller brottslig verksamhet i cybermiljö. Det kan t.ex. röra sig om underrättelseinformation om att en eller flera servrar kan komma att utnyttjas för att begå ett cyberangrepp eller information om att ett visst informationssystem har bekräftats ingå i ett anonymiseringsnätverk som misstänks användas i brottsligt syfte. Det är då viktigt att kartlägga om det i den brottsliga verksamheten förekommer kommunikation mellan informationssystemet i fråga och andra informationssystem.

Även Polismyndigheten har framhållit behovet av att kunna kartlägga kommunikation mellan informationssystem som misstänks utnyttjas i brottslig verksamhet i cybermiljö. Kriminella som opererar i cybermiljön använder sig enligt myndigheten inte alltid av enskilda informationssystem utan av omfattande digital infrastruktur, dvs. ett nätverk av informationssystem som samverkar med varandra. Exempel på det är marknadsplatser på Darknet som utnyttjas för bedrägerier, övergreppsnätverk och crime as a service. Den brottsliga verksamheten kan bedrivas från en server som finns i ett visst land, medan forum för diskussioner och allmän kundservice kan skötas via en server som finns i ett annat land och ett kund- och kontoregister kan finnas på en server i ett tredje land. Det är inte ovanligt att myndighetens första kontakt med illegal verksamhet av det här slaget är upptäckten av en av servrarna, samtidigt som myndigheten inte känner till de övriga. Ett ingripande mot en server kan medföra att det snabbt skapas en backup, som kan ligga på en server i ett fjärde land. Ingripandet får då inte avsedd effekt. För att göra ingripandet mer effektivt, t.ex. genom att samarbeta med brottsbekämpande myndigheter i andra länder, är det därför viktigt att kunna kartlägga den digitala infrastrukturen för den aktuella brottsligheten, i syfte att kunna ingripa mot hela eller den övervägande delen av brottsligheten.

Att ingripa mot informationssystem i syfte att kunna kartlägga digital infrastruktur som utnyttjas i brottslig verksamhet i cybermiljö bör enligt utredningens mening vara tillåtet. Det är emellertid

viktigt att framhålla att ett ingripande för det nu aktuella ändamålet inte är avsett att skapa underlag för att ansöka om preventiva tvångsmedel eller att ersätta möjligheten att använda sådana tvångsmedel. Utredningen återkommer till det i avsnitt 20.1.

Sammanfattningsvis anser utredningen att ett ändamål för ingripanden bör vara att tillfälligt bereda sig tillgång till trafikuppgifter under befordran för att kunna kartlägga om det i den brottsliga verksamheten förekommer kommunikation mellan ett informationssystem som kan antas utnyttjas i brott eller brottslig verksamhet och andra informationssystem.

14.2 Ingripanden för att hindra, störa eller avbryta

Utredningens förslag

Polismyndigheten, Säkerhetspolisen eller Tullverket får, om det behövs, bereda sig tillgång till informationssystem och till uppgifter i det i syfte att

1. ändra eller blockera uppgifter som ger tillgång till eller behandlas i informationssystemet, eller
2. genom annan liknande åtgärd störa eller hindra användningen av uppgifter som behandlas i informationssystemet.

Skälen för utredningens förslag

Utgångspunkter

En given utgångspunkt för den nya regleringen bör vara att den tillåter de brottsbekämpande myndigheterna att vidta sådana åtgärder som normalt faller under kriminaliseringen av dataintrång och som behövs för att uppnå de mål som anges i direktiven. Enligt 4 kap. 9 c § brottsbalken döms, som tidigare nämnts, den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift, för dataintrång. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Frågan är om de nya

befogenheterna bör omfatta allt från att bereda sig tillgång till uppgifter i informationssystem till att radera uppgifter.

En annan utgångspunkt för den nya regleringen bör vara att den så långt möjligt ska vara teknikneutral. Det är viktigt både eftersom brottsligheten i cybermiljö ständigt anpassas till de brottsbekämpande myndigheternas möjligheter att ingripa och med tanke på den snabba tekniska utvecklingen. Det innebär att det i lagen bör anges vilka slags åtgärder som får vidtas men inte närmare preciseras vilka tekniska hjälpmedel som får användas eller hur ingripandet rent tekniskt ska genomföras.

Åtgärder som i dag är straffbelagda

När det gäller frågan vilka typer av åtgärder som bör vara tillåtna för de brottsbekämpande myndigheterna att vidta är, som nyss nämnts, utgångspunkten att sådana åtgärder som anges i straffbestämmelsen om dataintrång ska kunna användas.

Bestämmelsen om dataintrång har sitt ursprung i 21 § i den upphävda datalagen (1973:289). Enligt den paragrafen dömdes ”den som olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning för dataintrång till böter eller fängelse i högst två år, om inte gärningen är belagd med straff i brottsbalken eller i lagen (1990:409) om skydd för företagshemligheter”. Med upptagning avsågs enligt paragrafen även uppgifter som var under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling. Enligt förarbetena var avsikten med straffbestämmelsen att den skulle omfatta alla obehöriga åtgärder i alla slag av dataregister, även sådana som inte innehöll personinformation, och oberoende av vilken information som åtgärden riktade sig mot (prop. 1973:33 s. 105).

Straffbestämmelsen kom senare att överföras till brottsbalken. För att uppfylla kraven i europeiska rådets rambeslut om angrepp mot informationssystem lades rekvisitet ”blockerar” och meningen ”Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift” till (prop. 2006/07:66 s. 1). När rambeslutet ersattes av EU-direktivet om angrepp mot informationssystem infördes ett nytt brott,

grovt dataintrång, med en strängare straffskala, för att uppfylla direktivets krav (prop. 2013/14:92 s. 13 f.).

En eller flera åtgärder?

Vid bedömningen av vilka typer av åtgärder som bör vara tillåtna vid ett ingripande i cybermiljö bör hänsyn tas till hur de brottsbekämpande myndigheternas behov närmare ser ut. Det är inte självklart att alla de åtgärder som ryms i straffbestämmelsen om dataintrång behöver användas vid varje ingripande. Samtidigt kan den ingripande myndigheten behöva använda flera av åtgärderna. Det kan bero på att det som myndigheten vill åstadkomma med ingripandet bara kan uppnås genom flera olika åtgärder tillsammans eller att flera åtgärder vidtas i olika steg för att åstadkomma den avsedda effekten.

I vissa fall kan ingripandet misslyckas, så att den förväntade effekten av åtgärden inte realiseras. Ett nytt beslut om ingripande kan då behöva fattas för samma eller en annan åtgärd för att uppnå den eftersträvade effekten. Vidare kan ett nytt beslut behöva fattas om en åtgärd endast delvis leder till den avsedda effekten och därför behöver kompletteras med någon annan typ av åtgärd.

Det är vidare tänkbart att samma effekt som ingripandet väntas få skulle kunna, helt eller delvis, uppnås med andra metoder. Utredningen återkommer till hur åtgärderna förhåller sig till bl.a. regleringen om hemliga tvångsmedel.

Bereda sig tillgång till

Som framgått av kapitel 11 behöver de brottsbekämpande myndigheterna kunna bereda sig tillgång till uppgifter i informationssystem utan att göra sig skyldiga till dataintrång. Det är nödvändigt för att de ska kunna upptäcka och så småningom ingripa mot brott och brottslig verksamhet i cybermiljö. Att bereda sig tillgång till ett informationssystem är normalt en förutsättning för att myndigheten ska kunna vidta ytterligare åtgärder i informationssystemet.

Begreppet bereda sig tillgång till innebär i detta sammanhang att myndigheten – oftast utan att den vars informationssystem eller uppgifter ingripandet riktas mot vet om det – genom en teknisk åtgärd eller på något annat sätt skaffar sig tillgång till hela eller delar

av ett informationssystem. På så sätt blir det möjligt för myndigheten att vidta ytterligare åtgärder (vilket utredningen återkommer till) i informationssystemet.

Av förarbetena till bestämmelsen om dataintrång framgår att det för straffansvar inte förutsätts att den som bereder sig tillgång till uppgifter avsedda för automatiserad behandling gör det i ett visst syfte eller att åtgärden i sig medför någon särskild effekt, t.ex. skada. Inte heller förutsätts det att någon säkerhetsåtgärd kringgås (prop. 2006/07:66 s. 17). Det saknar vidare betydelse för straffansvaret om tillgången bereds genom att besittningen till uppgifterna rubbas eller inte (prop. 1973:33 s. 105). Det är också tillräckligt att personen kan få del av uppgifterna. Det krävs inte att han eller hon verkligen tar del av dem (prop. 2006/07:66 s. 24).

Enligt bestämmelsen om dataintrång ska åtgärden rikta sig mot uppgifter avsedda för automatiserad behandling. Sådana hanteras, som tidigare nämnts, av informationssystem. Alla typer av uppgifter omfattas, dvs. fakta, information eller begrepp. Även dataprogram av olika slag omfattas. Det saknar betydelse var uppgifterna finns eller var de förvaras i systemet. Därmed innefattas också uppgifter som finns i en dators temporära minne. Även uppgifter som är under befordran omfattas av straffansvaret. Det senare gäller oavsett på vilket sätt de befordras, men det omfattar som regel inte uppgifter som befordras via radio (prop. 2006/07:66 s. 40 f. och 49).

När en myndighet bereder sig tillgång till ett informationssystem är det oundvikligt att tillgången ger möjlighet att ta del av uppgifter som behandlas i informationssystemet. Syftet med tillgången är dock i detta fall inte att ta del av innehållet utan framför allt att kunna lokalisera var den eller de uppgifter finns i systemet som ingripandet ska riktas mot. Det kan t.ex. handla om att myndigheten behöver söka igenom olika filer eller mappar på en dator för att ta reda på var brottsligt material lagras. Syftet med åtgärden är alltså inte att hämta in uppgifter i syfte att granska och analysera dem för att utreda brott eller förhindra viss brottslig verksamhet på det sätt som görs vid bl.a. hemlig dataavläsning (jfr Hemlig dataavläsning mot allvarliga brott, prop. 2024/25:51, s. 33). En fråga som i det här sammanhanget aktualiseras är hur ingripanden i cybermiljö förhåller sig till hemliga tvångsmedel. Utredningen återkommer till den frågan i avsnitt 20.1. Det är alltså viktigt att hålla isär åtgärden att bereda sig tillgång till uppgifter som ger tillgång till eller som behandlas i ett informations-

system och de eventuella åtgärder som vidtas därefter. Det kan t.ex. visa sig att informationssystemet saknade den anknytning till brott eller brottslig verksamhet som antogs vara fallet när beslutet om ingripande fattades.

Av tydlighetsskäl bör det framgå av den nya lagen att systemskydd får brytas eller kringgås och att tekniska sårbarheter får utnyttjas vid ett ingripande i cybermiljö. Utredningen återkommer till den frågan i avsnitt 18.2.

Enligt utredningens mening svarar innebörden av begreppet bereda sig tillgång till väl mot det behov som de brottsbekämpande myndigheterna har.

En förutsättning för att ett ingripande ska få göras bör vara att syftet med ingripandet endast kan uppnås genom den åtgärden. Myndigheten har normalt behov av att bereda sig tillgång till informationssystemet och uppgifter i det för att syftet med ingripandet ska uppnås. Några andra, mindre ingripande, åtgärder ska inte stå till buds. I undantagsfall kan ett ingripande göras utan att myndigheten behöver bereda sig tillgång till informationssystemet, t.ex. vid viss form av blockering.

Utredningen anser därför att de brottsbekämpande myndigheterna bör ha befogenhet att, om det behövs, bereda sig tillgång till ett informationssystem och till uppgifter i det i syfte att kunna ingripa i cybermiljö.

Ändra

Av förarbetena till bestämmelsen om dataintrång framgår att en ändring kan gälla de uppgifter som behandlas, men även dataprogram som styr den aktuella databehandlingen. Ändringen kan vara bestående eller tillfällig (prop. 2006/07:66 s. 18 f.). I förarbetena ansågs rekvisiten ändra eller utplåna motsvara de åtgärder som benämns skada, radera, försämra och ändra i artikel 3 i det rambeslut som föregick EU-direktivet om angrepp mot informationssystem. Det konstaterades samtidigt att rekvisiten i fråga i många fall även skulle kunna täcka in övriga åtgärder i artikeln, dvs. att mata in, överföra, hindra flödet av eller göra det omöjligt att komma åt uppgifter (prop. 2006/07:66 s. 26).

Med hänsyn till att ändringen ska röra uppgifter som är avsedda för automatiserad behandling omfattar straffbestämmelsen både att någon ändrar en befintlig uppgift som behandlas i ett informationssystem och att någon ändrar en uppgift under befordran till informationssystemet.

Som framgått av kapitel 11 behöver de brottsbekämpande myndigheterna kunna ändra information i olika typer av informationssystem, bl.a. digitala plattformar och tjänster. Det är framför allt fråga om att kunna ändra uppgifter som ger tillgång till ett visst informationssystem eller en viss del av det. Myndigheterna har t.ex. behov av att kunna ta över en webbplats genom att byta lösenord eller att ta över en server eller en plattform som utnyttjas för brottslig aktivitet genom att utestänga den som äger eller använder den från teknisk tillgång till den. Myndigheterna kan även behöva ändra andra uppgifter som ger tillgång till informationssystemet, t.ex. genom att använda ett virtuellt privat nätverk (Virtual Private Network, VPN).

Att ändra innebär alltså i detta sammanhang i första hand att information tillfälligt görs otillgänglig, t.ex. att informationen krypteras. Det kan också innebära att påverka uppgifter som redan behandlas i informationssystemet när myndigheten ingriper eller att nya uppgifter förs in för att åstadkomma ett visst resultat.

Till skillnad från det som gäller enligt straffbestämmelsen om dataintrång bör i detta sammanhang endast ändringar som innebär att den som äger eller använder ett informationssystem tillfälligt avhänds rådigheten över vissa uppgifter omfattas av begreppet ändra. Det innebär att den ingripande myndigheten ska göra det möjligt för den, vars informationssystem eller uppgifter ett ingripande har riktats mot, att återfå rådigheten över dem genom att myndigheten t.ex. tar bort kryptering, tillhandahåller en kopia av uppgifterna i fråga eller ser till att den berörde genom att byta lösenord på nytt kan få tillgång till sina uppgifter. Utredningen återkommer i avsnitt 14.5.2 till frågan om ändringar av oåterkallelig karaktär. Myndigheterna har endast behov av att ändra uppgifter som ger tillgång till ett informationssystem eller som redan behandlas i det. Uppgifter under befordran till informationssystem bör alltså inte få ändras, såvida det inte är fråga om uppgifter som ändrar tillgången till systemet. Ett försök att kryptera informationen, byta ut lösenordet eller vidta någon annan åtgärd för att hindra att brottsbekämpande myndigheter får

tillgång till systemet och informationen där, bör alltså kunna mötas med motåtgärder. Däremot bör möjligheten att ändra uppgifter som ger tillgång till ett informationssystem inte få användas för att löpande kunna följa verksamheten i systemet, eftersom det innebär att regelverket för hemliga och preventiva tvångsmedel då kringgås.

Sammanfattningsvis anser utredningen att de brottsbekämpande myndigheterna bör ha befogenhet att bereda sig tillgång till informationssystem och till uppgifter i systemet i syfte att ändra uppgifter som antingen ger tillgång till eller behandlas i informationssystemet.

Blockera

I förarbetena till straffbestämmelsen om dataintrång ansågs förfaranden som att hindra flödet av eller göra det omöjligt att komma åt uppgifter enligt artikel 4 i det rambeslut som föregick EU-direktivet om angrepp mot informationssystem inte fullt ut täckas av den då gällande straffbestämmelsen om dataintrång. Sådana åtgärder som föll utanför ansågs kunna bestå i hindrande eller spärrande åtgärder av olika slag och införande eller spridning av olika typer av sabotageprogram (exempelvis datavirus, trojaner eller logiska bomber) som gör att uppgifterna blockeras. Det ansågs vidare kunna handla om situationer där en programkod förs in i en dator som fyller minnesutrymmet med skräppost, så att uppgifterna i informationssystemet inte kan nås eller som gör att uppgifterna inte kan lokaliseras. Straffansvaret för dataintrång utvidgades därför till att även omfatta den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling (prop. 2006/07:66 s. 41 f. och 50). För straffansvar krävs inte att blockeringen medför ett avbrott eller annars allvarligt hindrar systemets drift (prop. 2006/07:66 s. 43 f.).

Som framgått av kapitel 11 behöver de brottsbekämpande myndigheterna kunna påverka tillgängligheten till digitala plattformar, tjänster, andra informationssystem och nätverksanslutna enheter genom att blockera digital kommunikation eller it-infrastruktur till t.ex. en webbplats eller ett användarkonto, för att på så sätt förhindra att kommunikationen når fram. Vidare kan myndigheterna behöva blockera uppgifter som ger tillgång till informationssystemet, t.ex. genom att VPN används.

Som exempel på situationer där blockering enligt utredningens mening kan bli aktuell kan nämnas att blockera olika enheter som ingår i ett ransomewareangrepp för att begränsa eller avvärja angreppet, att blockera tillgången till uppgifter som innehåller övergreppsmaterial som rör barn eller att blockera tillgången till information om hur illegala droger eller vapen kan anskaffas.

Olika former av åtgärder som innebär att uppgifter i ett informationssystem blockeras är inte, till skillnad från radering, av oåterkallelig karaktär. Att blockera uppgifter i ett informationssystem bör därför anses vara en mindre ingripande åtgärd än att radera uppgifter. Intrånget för den enskilde och den eventuella skadan på uppgifterna i informationssystemet kan variera beroende på hur blockeringen görs. Blockering kan åstadkommas med hjälp av t.ex. en programkod som möjliggör att den enskilde vars informationssystem eller uppgifter som ett ingripande har riktats mot vid behov senare kan återfå rådigheten över uppgifterna. Blockering kan i vissa fall även åstadkommas med hjälp av ett sabotageprogram. Utgångspunkten bör vara att minsta möjliga skada ska uppkomma vid ingripandet.

Blockering kan förväntas bli ett mycket viktigt verktyg för myndigheterna för att kunna ingripa mot brott och brottslig verksamhet i cybermiljö. Ett exempel kan vara att uppgifterna finns på en server som är oåtkomlig för svenska myndigheter, och därför inte kan raderas, men där det skulle finnas viss möjlighet att blockera tillgången till uppgifterna. Blockering är då den enda möjliga åtgärden. Med hänsyn till det anser utredningen att de brottsbekämpande myndigheterna bör ha befogenhet att bereda sig tillgång till informationssystem och till uppgifter i sådana system i syfte att blockera uppgifter som ger tillgång till eller behandlas i informationssystemet.

Vid blockering kan det finnas situationer där det, när tiden för den ursprungliga åtgärden löper ut (se avsnitt 17.1.2), står klart att blockeringen behöver fortsätta att gälla (t.ex. vid blockering av en marknadsplats som erbjuder förbjudna droger). Då kan, om förutsättningarna enligt lagen fortfarande är uppfyllda, ett nytt beslut om blockering fattas.

Beroende på hur långvarig en blockering blir, kan det diskuteras om ingripandet inte kan jämställas med radering. Utredningen vill betona att kortvariga blockeringar, som det i många fall kommer att röra sig om, knappast innebär ett större intrång i den personliga integriteten än andra ingripanden som görs i den brottsbekämpande

verksamheten. Om blockeringen sträcker sig över längre tid än den som maximalt får användas för att genomföra ett ingripande, dvs. en månad, kommer det att krävas ett nytt beslut, där frågan om åtgärden är proportionerlig, ska prövas. Om det inte längre finns skäl för blockeringen ska beslutet alltid upphävas (se avsnitt 18.5). De bestämmelserna tillsammans innebär enligt utredningens mening tillräckliga garantier för att blockering ska vara en godtagbar åtgärd.

Allvarligt hindra eller störa

Förfaranden som allvarligt hindrar eller avbryter driften av ett informationssystem genom bl.a. inmatning eller överföring av datorbehandlingsbara uppgifter, enligt artikel 3 i det rambeslut som föregick EU-direktivet om angrepp mot informationssystem, ansågs enligt förarbetena inte täckas av straffbestämmelsen om dataintrång i dess dåvarande lydelse. Det konstaterades att det finns situationer där program skapar och sänder så stora mängder e-post att mottagarens system kollapsar eller får kraftigt nedsatt funktion och som därmed allvarligt stör eller hindrar användningen av de uppgifter som behandlas i systemet, utan att uppgifterna i informationssystemet helt blockeras. Det kan innebära att tillgången till uppgifterna begränsas mycket kraftigt, utan att möjligheterna att använda systemet helt spolieras. En sådan effekt kan också enligt förarbetena uppkomma till följd av manuella sändningar av e-post i stor skala. Som ytterligare exempel på åtgärder som kan verka på ett sådant sätt nämndes upprepade anrop eller försök till anrop och införing av virusprogram eller annat sabotageprogram. För att få en mer heltäckande reglering lades meningen ”Detsamma gäller den som olovligen genom någon liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift” till i straffbestämmelsen. Effekten av åtgärden ska alltså påverka den normala användningen av uppgifterna kraftigt. För straffansvar krävs att det är frågan om betydande störningar av inte endast tillfällig natur. Med begreppet hindrar avses fall där användningen av en uppgift som är avsedd för automatiserad behandling helt avbryts eller hindras. I det senare fallet torde dock som regel ansvar i stället inträda för blockering (prop. 2006/07:66 s. 44 och 50 f.).

Som framgått av kapitel 11 behöver de brottsbekämpande myndigheterna kunna påverka tillgången till bl.a. digitala plattformar,

tjänster, andra informationssystem och nätverksanslutna enheter, genom t.ex. ett överbelastningsangrepp eller genom att stänga ner ett användarkonto eller en webbplats. Det kan t.ex. vara nödvändigt för att förhindra att samhällsviktig information överförs till en antagonistisk mottagare.

Enligt utredningens mening bör de brottsbekämpande myndigheterna kunna ingripa med andra åtgärder än ändring och blockering av uppgifter som behandlas av ett informationssystem, under förutsättning att det är fråga om liknande åtgärder. Det kan t.ex. vara överbelastningsangrepp eller införing av program som leder till att användningen av uppgifter som behandlas i informationssystem störs eller hindras. I bestämmelsen om dataintrång straffbeläggs endast allvarligt störande. Ett ingripande enligt den nya lagen ska alltid vara proportionerligt och den minst ingripande sättet att genomföra det bör väljas. I det här sammanhanget saknar det därför betydelse om störningen skulle anses vara allvarlig eller inte.

Sammanfattningsvis anser utredningen att de brottsbekämpande myndigheterna bör ha befogenhet att bereda sig tillgång till informationssystem och till uppgifter i det i syfte att – genom någon annan liknande åtgärd än att ändra eller blockera – störa eller hindra användningen av uppgifter som behandlas i informationssystemet.

Föra in i register

Som tidigare nämnts infördes straffbestämmelsen om dataintrång ursprungligen i den numera upphävda datalagen, som huvudsakligen innehöll bestämmelser som syftade till att förebygga otillbörligt integritetsintrång genom registrering. Flertalet bestämmelser reglerade register som innehöll personinformation, men lagen innehöll även bestämmelser som var tillämpliga på all slags datalagrad information (prop. 1973:33 s. 114 f.). Det var efter kritik från Justitiekanslern som även förfarandet att någon olovligen för in upptagning i ett register lades till bland det straffbara handlandet, även om det enligt Justitiekanslern möjligen kunde hävdas att en införing innebär ändring av en upptagning (prop. 1973:33 s. 68 och 105 f.). Här kan noteras att olika begrepp som datasystem, register och dataregister användes i övervägandena, även om begreppet register var det som kom att användas i författningstexten.

Enligt 1 § datalagen definierades personregister som register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften. I förarbetena uttalades följande (prop. 1973:33 s. 118).

> För att ett register ska anses föreligga måste det direkt eller indirekt vara fråga om behandling från informationssynpunkt av faktiska uppgifter. Ett ADB-register kan sålunda inte anses upprättat bara genom att löpande text lagras i ett datamedium, exempelvis för att sättning ska kunna ske med hjälp av ADB-teknik. Uppenbarligen faller på grund härav åtskillig databehandling av olika slags litteratur, främst skönlitteratur, utanför datalagens tillståndssystem. Först i den mån databehandlingen tar sikte på faktiska uppgifter i den litterära framställningen – såsom för upprättande av innehållsregister eller liknande – föreligger ett register i datalagens mening. Vidare bör ett register anses föreligga, om de lagrade uppgifterna ska användas för att framställa exempelvis en telefonkatalog, ett adressregister eller en taxeringskalender. Den närmare gränsdragningen när det gäller att bestämma registerbegreppets innebörd får göras i praxis.

Den numera upphävda personuppgiftslagen (1998:204), som ersatte datalagen, innehöll inga bestämmelser som byggde på begreppet register.

Av förarbetena till ändringar i straffbestämmelsen om dataintrång framgår att Rikspolisstyrelsen under remissbehandlingen ifrågasatte den nu aktuella kriminaliseringen och ansåg att begreppet register borde utgå. Enligt Rikspolisstyrelsen medförde begreppet att det straffbara området blev för snävt, eftersom informationen för att omfattas måste vara strukturerad på ett visst sätt. Genom att slopa orden ”i register” skulle enligt Rikspolisstyrelsen bestämmelsen bli tydligare och diskussioner om vilket skydd uppgifter ordnade i register ska åtnjuta i förhållande till andra uppgifter inte behöva uppkomma (prop. 2006/07:66 s. 18).

Regeringen noterade att begreppet ”föra in i register” tillkom när datalagen infördes men att någon närmare diskussion om kriminaliseringens innebörd i den delen inte fördes (prop. 2006/07:66 s. 46). Regeringen konstaterade att begreppet register medför en begränsning av det straffbara området så till vida att endast sådana införingar som görs i uppgifter strukturerade på visst sätt omfattas (a. prop. s. 18). Det var enligt regeringen svårt att föreställa sig en situation där en införing görs i något som inte är ett register och där införingen

inte heller i övrigt omfattades av kriminaliseringen i dataintrångsbestämmelsen. Det hade inte heller framförts någon direkt kritik mot bestämmelsen med hänsyn till tillämpningen i praxis. Att slopa begreppet register riskerade enligt regeringens mening att medföra en alltför vidsträckt kriminalisering. Behovet av att utvidga dataintrångsbestämmelsen till att omfatta alla införingar framstod således av flera skäl enligt regeringen som tveksamt, varför en sådan ändring inte borde genomföras (a. prop. s. 47).

Som framgått av kapitel 11 behöver de brottsbekämpande myndigheterna kunna lägga till information i olika typer av informationssystem. De brottsbekämpande myndigheterna har emellertid inte påtalat något behov av att vidta åtgärder som riktar sig mot någon form av register. Det kan konstateras att den digitala tekniken i dag är uppbyggd så att olika uppgifter förs samman med varandra från olika informationssystem. Begreppet register får därför anses vara otidsenligt.

Användningen av begreppet register i straffbestämmelsen om dataintrång innebär att det straffbara området avgränsas genom att det inte är tillåtet att föra in uppgifter i ett informationssystem som är strukturerat på ett visst sätt. Det innebär samtidigt att det är tillåtet att föra in uppgifter i informationssystem som inte är strukturerade på sådant sätt att de är att anse som ett register, så länge införingen inte utgör något annat straffbart handlande, t.ex. ändring.

Även om det i framtiden skulle kunna uppstå behov för de brottsbekämpande myndigheterna av att kunna föra in uppgifter i register i den mening som avses i straffbestämmelsen om dataintrång, bör det enligt utredningens mening inte göras någon skillnad mellan åtgärderna ändra och föra in i den nya regleringen. Myndigheternas behov i den här delen bör därför rymmas inom begreppet ”ändra” uppgifter.

14.3 Ingripanden för att kartlägga brottslig verksamhet

Utredningens förslag

Om det kan antas att ett informationssystem utnyttjas i brott eller brottslig verksamhet i cybermiljö får Polismyndigheten,

Säkerhetspolisen eller Tullverket tillfälligt bereda sig tillgång till trafikuppgifter under befordran till eller från informationssystemet för att kunna kartlägga om det i den brottsliga verksamheten förekommer kommunikation med andra informationssystem.

Skälen för utredningens förslag

Kartlägga kommunikation mellan informationssystem

Säkerhetspolisen har särskilt lyft behovet av att kunna kartlägga kommunikation till och från informationssystem, s.k. noder som kan ingå i anonymiseringsnätverk (se avsnitt 11.2). Det kan exempelvis vara webbkameror eller wifiroutrar. Även Polismyndigheten har framhållit behovet av att kunna kartlägga digitala kommunikationsflöden, i syfte att få en bättre överblick över digital infrastruktur som används i brottslig verksamhet.

Som framgått av avsnitt 14.1.2 är ändamålet med en sådan åtgärd att upptäcka – alternativt verifiera eller utesluta – om informationssystemen utnyttjas för brott eller i brottslig verksamhet. Det skulle göra det möjligt att kartlägga och analysera den brottsliga verksamheten, i syfte att – vid rätt tidpunkt – kunna störa och avbryta den. För att kunna utnyttja möjligheten att få tillgång till sådana trafikuppgifter behöver de brottsbekämpande myndigheterna kunna begära medverkan av de verksamhetsutövare som har rådighet över den aktuella nätverkstrafiken, t.ex. teleoperatörer, internetleverantörer och olika datacenter. Utredningen återkommer till det i avsnitt 18.4.

Tillämpningsområdet för ingripandet bör begränsas på det sättet att det ska finnas viss misstanke om att informationssystemet faktiskt utnyttjas i brott eller brottslig verksamhet. Kravet bör emellertid vara lågt ställt. Det bör räcka att det kan antas att informationssystemet utnyttjas på det sättet. Man kan också uttrycka det så att det ska finnas någon faktisk omständighet som talar för att informationssystemet i fråga har en roll i den misstänkta digitala infrastrukturen. Det innebär att ingripanden inte kan riktas mot informationssystem där det helt saknas kunskap om hur de används.

Det rör sig om kortvariga ingripanden som görs för att kartlägga om det förekommer kommunikation mellan olika informationssystem, för att den brottsbekämpande myndigheten ska kunna avgöra om de utnyttjas i brott eller brottslig verksamhet eller inte

och, om möjligt, för att kunna identifiera det informationssystem som ett brottsligt cyberangrepp ursprungligen härrör från.

Syftet med den nu aktuella åtgärden är att, genom ingripandet, bl.a. kunna börja nysta upp anonymiseringsnätverk som utnyttjas för illegala syften. Ingripandet syftar alltså inte till att löpande följa trafiken till och från informationssystemet, utan enbart till att – vid ett tillfälligt ingripande – kunna upptäcka vilken roll det kan ha eller ha haft i nätverket. Om det vid ingripandet kan konstateras att ett visst informationssystem ingår eller har ingått i ett anonymiseringsnätverk kan det i enskilda fall finnas förutsättningar för att använda preventiva tvångsmedel för att utreda frågan vidare. Det kan också innebära att det finns grund för att vidta andra åtgärder enligt den nu aktuella lagen, t.ex. att blockera tillgången eller att radera en skadlig kod.

Slutsats

Sammanfattningsvis anser utredningen att de brottsbekämpande myndigheterna bör ha befogenhet att, om kan antas att ett informationssystem utnyttjas i brott eller brottslig verksamhet i cybermiljö, tillfälligt bereda sig tillgång till trafikuppgifter under befordran till eller från informationssystemet för att kunna kartlägga om det i den brottsliga verksamheten förekommer kommunikation med andra informationssystem.

14.4 Krav på särskild vikt

Utredningens förslag

För ingripanden för att förhindra eller avbryta brott eller störa eller avbryta brottslig verksamhet eller kartlägga kommunikation mellan informationssystem som kan antas utnyttjas i brott eller brottslig verksamhet ska det krävas att ingripandet är av särskild vikt.

Skälen för utredningens förslag

Det bör av rättssäkerhetsskäl ställas krav på ingripandets förväntade betydelse för brottsbekämpningen. En förutsättning för ett ingripande i cybermiljö bör vara att det på sakliga grunder kan bedömas att ingripandet skulle ha betydelse för det ändamål för vilket det vidtas. För en sådan bedömning krävs att den information som finns tillgänglig ger vid handen att en sådan effekt kan förväntas. Det bör uttryckas så att ett ingripande får göras om det är av särskild vikt för att förhindra eller avbryta brott eller störa eller avbryta brottslig verksamhet i cybermiljö. Kravet på särskild vikt innefattar både ett kvalitetskrav avseende den effekt som åtgärden kan ge och ett krav på behovet av ingripandet i det enskilda fallet. Bedömningen att ingripandet är av särskild vikt får inte bygga enbart på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter som talar för att den avsedda effekten kan uppnås (jfr De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation, prop. 2011/12:55, s. 121). Särskild vikt är ett lägre krav än synnerlig vikt. Enligt utredningens mening skulle ett krav på att ingripandet ska vara av synnerlig vikt för det syfte i vilket det görs innebära ett för högt ställt krav sett i förhållande till det behov och den nytta som ingripanden i cybermiljö kan förväntas få. Utredningen återkommer dock till frågan om det kravet när det gäller radering.

14.5 Särskilt om radering

14.5.1 Innebörden av radering

Som framgått ansågs rekvisiten ändra eller utplåna i förarbetena till straffbestämmelsen om dataintrång motsvara de åtgärder som benämns skada, radera, försämra och ändra i artikel 3 i det rambeslut som föregick EU-direktivet om angrepp mot informationssystem (prop. 2006/07:66 s. 26). Vidare framgår av förarbetena att utplåning innebär att en uppgift avsedd för automatiserad behandling helt eller delvis förstörs, t.ex. genom radering (a. prop. s. 18). I de fall där ett program förs in i en dator och fyller minnesutrymmet med ”skräp” så att uppgifterna förändras eller förstörs kan ansvar för dataintrång komma i fråga för ändring eller utplånande av dem (a. prop. s. 50).

Som framgått av kapitel 11 anser de brottsbekämpande myndigheterna att de i vissa fall behöver kunna radera lagrad information i olika typer av informationssystem, t.ex. information på delar av digitala plattformar och tjänster.

Inledningsvis vill utredningen framhålla att begreppet radera, som bör användas, är ett mer tidsenligt begrepp än begreppet utplåna som används i straffbestämmelsen om dataintrång. Att begreppet utplåna i straffbestämmelsen kan ha ett något vidare tillämpningsområde och även kan omfatta t.ex. fysisk förstöring saknar enligt utredningens mening betydelse i det här sammanhanget.

Både begreppet radera och begreppet utplåna kan ge intryck av att viss information avlägsnas fullständigt. Så blir emellertid inte alltid fallet i cybermiljö. Det som förstörs vid radering är den kända informationen i ett eller flera informationssystem. Det kan emellertid inte uteslutas att det finns kopior av samma information i andra system, eftersom digital information är så enkel att kopiera. En radering i digital miljö kan därmed inte garanteras ha samma slutliga effekt som när något förstörs i fysisk miljö.

14.5.2 Radering bör i vissa fall vara en tillåten åtgärd

Utredningens förslag

Om det är av synnerlig vikt för att förhindra eller avbryta brott i cybermiljö får Polismyndigheten, Säkerhetspolisen eller Tullverket radera uppgifter som behandlas i ett informationssystem som myndigheten har berett sig tillgång till med stöd av den nya lagen.

Skälen för utredningens förslag

Radering ska endast vara tillåten i vissa fall

Utredningen anser att det bland de tillåtna ingripandena även bör ingå att kunna radera uppgifter som behandlas i ett informationssystem. Det kan t.ex. bli aktuellt att radera övergreppsmaterial så att spridning av barnpornografi inte kan fortgå, eller att ta bort en skadlig programvara på nätverksanslutna enheter för att förhindra att de kan utnyttjas för brott i framtiden. Radering av uppgifter i ett infor-

mationssystem är – till skillnad från blockering – en åtgärd av oåterkallelig karaktär. Det saknar betydelse om uppgifterna även finns i andra informationssystem eller om det finns kopior av dem i fysisk form. Det är således endast uppgifterna som ingripandet riktar sig mot som ska hanteras så att de inte kan återställas i det aktuella informationssystemet, för att åtgärden ska utgöra radering enligt lagen. Det kan t.ex. vara fråga om att radera uppgifter som lagras i ett informationssystem som har använts för att stjäla uppgifter från ett företag eller en myndighet. Det saknar betydelse om företaget eller myndigheten har kvar motsvarande uppgifter i ett informationssystem som används för backup, eftersom det är uppgifterna som lagras i det informationssystem som har använts som ett hjälpmedel för brott, dvs. för att stjäla uppgifterna eller senare lagra dem, som ska raderas.

Det är en principiell skillnad mellan radering och ingripanden som endast innebär att uppgifter tillfälligt ändras, blockeras eller på annat sätt störs eller hindras från normal användning. Med hänsyn till att radering är en oåterkallelig åtgärd ligger det i sakens natur att åtgärden kan orsaka värre skada eller utgöra ett större integritetsintrång för den vars uppgifter blir föremål för radering än en åtgärd som innebär att den enskilde kan återfå rådigheten över uppgifterna. Det finns därför skäl att omgärda radering med särskilda rättssäkerhetsgarantier. Det bör ställas högre krav på förutsättningarna för radering än det som gäller för andra ingripanden enligt den nya lagen. Det bör även ställas högre krav på den som beslutar om radering, se avsnitt 16.2.1.

Som utredningen har påpekat i avsnitt 14.2 är en brottsbekämpande myndighets byte av lösenord, i syfte att bereda sig tillgång till uppgifter som behandlas i ett informationssystem, inte att betrakta som radering i den nya lagens mening. Det beror på att den som genom lösenordsbytet tillfälligt berövas rådigheten över systemet har möjlighet att senare, genom ett nytt lösenordsbyte, återfå rådigheten och antingen återanvända det gamla lösenordet eller skapa ett nytt.

Bör radering få användas för att förebygga brott?

En särskild fråga när det gäller radering är om den åtgärden, till skillnad från övriga åtgärder enligt den nya lagen, även bör få användas för att förebygga brott. Utredningen har övervägt det, mot bakgrund av att vissa brott i cybermiljö begås systematiskt eller genererar material som är särskilt integritetskränkande. En möjlighet att radera sådant material redan i samband med ingripandet i cybermiljö skulle i vissa fall onekligen innebära en fördel för målsäganden, t.ex. om det är fråga om bilder som visar honom eller henne i en förnedrande situation, eftersom utredning och lagföring kan ta lång tid. Det gäller inte minst om det krävs internationellt samarbete för att genomföra brottsutredningen. Utredningen anser emellertid att en sådan ordning inte bör införas, eftersom det skulle kunna äventyra möjligheterna att lagföra den som ligger bakom brottet. Vidare bör beaktas att radering kan vara en åtgärd som aktualiseras senare, när en behörig myndighet har tagit ställning till frågan om förundersökning och åtal. Att förebygga brott bör därför inte vara en grund för radering enligt den nya lagen.

Förutsättningarna för radering

Ett första krav som bör ställas är att situationen gör radering nödvändig (jfr prop. 2005/06:177 s. 87 f.). Avgörande för om åtgärden är nödvändig bör vara hur stor skada som brottet eller den brottsliga verksamheten kan orsaka om uppgifterna inte raderas. Vidare bör åtgärden komma i fråga först i de situationer där andra mindre ingripande åtgärder, t.ex. blockering, inte bedöms vara tillräckliga för att uppnå syftet med åtgärden. Det kan exempelvis vara fråga om att en brottsbekämpande myndighet blockerar tillgången till en marknadsplats för illegala varor eller tjänster för utomstående, och därigenom förhindrar fortsatt brottslighet, i stället för att radera uppgifterna på marknadsplatsen. Så länge de som står bakom marknadsplatsen inte har identifierats och bevismaterial som kan användas för lagföring har säkrats, kan blockering vara en lämpligare åtgärd än radering.

Det ska vidare finnas skäl att räkna med att raderingen ensam eller i förening med andra åtgärder kan få avsedd effekt. Situationen kan vara den att blockering tillfälligt kan uppnå den avsedda effekten med ingripandet och därför bör komma i fråga i första hand, men att

radering senare bedöms vara nödvändig för att få till stånd en slutlig lösning. Det kan t.ex. handla om ett pågående barnpornografibrott, där myndigheten kan blockera den misstänkte från att ha tillgång till sitt informationssystem, vilket tillfälligt hindrar fortsatt brottslighet, men där en radering av det barnpornografiska materialet anses vara nödvändig för att förhindra att nya barnpornografibrott begås genom senare spridning av materialet.

Hänsyn måste också tas till vilka uppgifter det är fråga om. Radering bör kunna aktualiseras i såväl situationer där nya brott i cybermiljö kan förhindras som i situationer där pågående brott i cybermiljö kan avbrytas. Det kan röra sig om planer på terroristbrott, där brott kan förhindras genom att terrorisminnehåll raderas eller om att säkerhetskänslig information raderas för att förhindra eller avbryta spioneri eller olovlig underrättelseverksamhet. Det kan även röra sig om en skadlig kod som raderas för att förhindra eller avbryta pågående brott mot människors liv och hälsa eller egendom.

Även omfattningen av det som ska raderas har betydelse. Det kan i vissa fall vara tusentals filer eller bilder. Men det kan även, som tidigare nämnts, vara fråga om att radera någon enstaka bild eller film.

Eftersom radering är en åtgärd som är avsedd att vara oåterkallelig bör radering inte få användas i syfte att störa eventuellt pågående brottslig verksamhet.

Synnerlig vikt

Med hänsyn till åtgärdens ingripande karaktär bör det ställas högre krav för beslut om radering än för andra åtgärder som får användas vid ingripanden i cybermiljön. Enligt utredningen kommer det lämpligast till uttryck genom att det föreskrivs att radering får beslutas endast om åtgärden är av synnerlig vikt för att förhindra eller avbryta brott i cybermiljö. Med synnerlig vikt avses att det ska vara mycket svårt, eller rent av omöjligt, att åstadkomma samma resultat genom någon annan åtgärd. Som exempel kan nämnas att radering av bilder från kränkande fotografering i vissa fall kan vara den enda åtgärd som är möjlig att vidta för att förhindra att bilderna sprids.

Alternativa åtgärder

I vissa fall kan alternativ till radering komma i fråga. Möjligheten att förmå systemägare att avlägsna eller göra innehåll online som syftar till att rekrytera personer för att begå brott oåtkomligt, kan t.ex. övervägas i stället för radering (se 5 § förslaget till lag om avlägsnande av rekryteringsinnehåll online i prop. 2025/26:276). Vidare bör möjligheten att förmå den som tillhandahåller en elektronisk anslagstavla att ta bort visst innehåll enligt lagen om ansvar för elektroniska anslagstavlor beaktas. Detsamma gäller möjligheten att förmå värdtjänstleverantörer att avlägsna eller göra terrorisminnehåll eller innehåll som rör våld mot kvinnor och våld i nära relationer online oåtkomligt enligt TCO-förordningen och enligt direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Det bör enligt utredningens mening inte ställas något formellt krav på att alla andra tänkbara åtgärder alltid måste uttömmas innan ett beslut om radering aktualiseras. De måste emellertid alltid övervägas som ett led i proportionalitetsbedömningen. Om en kontakt med systemägare eller tillhandahållare av elektroniska anslagstavlor skulle riskera att avslöja polisens arbetsmetoder eller på annat sätt äventyra den brottsbekämpande verksamheten, bör beslut om radering kunna fattas ändå.

Förhållandet mellan radering och kopior

Det finns situationer där radering av de allra flesta skulle uppfattas som en närmast självklar åtgärd, där integriteten för den som åtgärden riktas mot får anses vara mindre skyddsvärd och radering därför är försvarbar. Utredningen tänker på den situationen där en mobiltelefon, dator eller annan kommunikationsutrustning innehåller exempelvis nakenbilder av en målsägande eller barnpornografi. Så länge som materialet finns i digital form är det lätt att både kopiera och sprida till andra. Även om det i en förundersökning inte går att styrka att den som innehar kommunikationsutrustningen har gjort sig skyldig till brott bör det vara möjligt att radera materialet i syfte att förhindra framtida brott i cybermiljö i form av sexualbrott, utpressning eller annat brott. Det behöver emellertid inte bara vara fråga om material med sexuellt färgat innehåll. Det kan även vara fråga om stulna uppgifter, t.ex. stulna personuppgifter, kontokorts-

uppgifter eller företagshemligheter som inte bör komma i orätta händer. Även radering av bilder eller filmer där någon avsiktligt förnedras eller uppenbart tvingas medverka till något mot sin vilja kan aktualiseras. Hot om att sprida sådant material används ibland mot yngre personer, i syfte att förmå dem att begå brott. Sådana hot används även av vissa män för att förmå kvinnor som vill lämna förhållanden att avstå från att göra det. Enligt utredningens mening kan en bestämmelse som ger brottsbekämpande myndigheter möjlighet att radera den typen av material bidra till ökad trygghet i samhället.

Exemplen aktualiserar en annan fråga, nämligen hur den brottsbekämpande myndighet, som anser att visst material bör raderas, bör hantera det förhållandet att det kan finnas kopior av det på lagringstjänster eller i andra informationssystem. Det bör emellertid inte ställas något krav på att eventuella kopior måste eftersökas.

Det är också viktigt att framhålla att frågan om radering kan te sig mer eller mindre angelägen, beroende på om den brottsbekämpande myndigheten vet om att ett flertal kopior finns i omlopp (här bortses från eventuella arbetskopior som myndigheten själv har framställt). Ju fler kopior som är kända, desto sämre bör förutsättningarna vara att få en slutlig lösning genom radering.

14.6 Ingripanden får endast avse brott eller brottslig verksamhet av viss svårhetsgrad

Utredningens förslag

Ett ingripande får endast avse brott för vilket det är föreskrivet fängelse i ett år eller mer, eller brottslig verksamhet som innefattar sådant brott, som begås eller kommer att begås i cybermiljö med hjälp av informationssystem.

Skälen för utredningens förslag

Tillämpningsområdet bör begränsas

Att myndigheter bereder sig tillgång till informationssystem som används av enskilda kan, som framgått av avsnitt 12.4, i ett enskilt fall leda till integritetsintrång som har likheter med de intrång som

användning av hemliga tvångsmedel medför. Utöver kravet på att ingripanden bara får beslutas för vissa ändamål (se avsnitt 14.1.2) anser utredningen därför att tillämpningsområdet för ingripandena bör begränsas ytterligare.

Enligt utredningens mening är det inte lämpligt att utforma en sådan begränsning genom att knyta an till någon misstanke mot person, eftersom åtgärderna riktar sig mot informationssystem eller delar av sådana. Även om det alltid finns en eller flera personer som äger eller använder ett informationssystem kan de många gånger vara okända för de brottsbekämpande myndigheterna. Den som ligger bakom brottslighet väljer ofta aktivt att utnyttja det faktum att brott i cybermiljö är svåra att koppla till någon person. I andra fall, t.ex. när ett informationssystem har utsatts för dataintrång, är den som äger eller använder systemet oftast ovetande om att det utnyttjas som ett brottsverktyg av någon annan. Som tidigare nämnts kan brott i cybermiljö avse en mängd olika företeelser. För att ge de brottsbekämpande myndigheterna möjlighet att ingripa mot de nu aktuella brotten, bör användningen av åtgärderna lämpligen, på samma sätt som gäller för de flesta tvångsmedel, endast få användas vid brott och brottslig verksamhet som innefattar brott av viss svårhetsgrad. Det är varken rimligt ur ett integritetsperspektiv eller resurseffektivt att ingripa enligt lagen vid mindre allvarliga brott eller vid störningar av allmän ordning och säkerhet som inte utgör brott. Frågan är då hur en sådan reglering närmare bör utformas.

En begränsning som utesluter mindre allvarliga brott

Det finns många sätt att avgränsa tillämpningsområdet på. För flertalet åtgärder som får vidtas i en förundersökning ställs det krav på brott av viss svårhetsgrad. Ofta ställs det också krav på viss brottsmisstanke, men det senare är inte någon rimlig avgränsning om ingripanden i cybermiljö ska kunna göras även på underrättelsestadiet. För t.ex. alla hemliga tvångsmedel, med undantag av postkontroll, avgränsas tillämpningsområdet genom en kombination av straffskalans nedre gräns och en brottskatalog som tar upp vissa brott som har ett lägre minimistraff. En brottskatalog skapar en klar och förutsebar gräns för tillämpningen, samtidigt som det synliggör integritetsavvägningen i lagtexten. Det krävs dock att brottskatalogen

kontinuerligt ses över i takt med att lagstiftningen förändras. En brottskatalog riskerar också att bli omfattande och svåröverskådlig.

Utredningen anser, med hänsyn till det nyss sagda, att en lämplig lösning är att avgränsa tillämpningsområdet genom att ange att ett ingripande endast får avse brott för vilket det är föreskrivet fängelse i ett år eller mer. Det avgörande är alltså om fängelsestraff av den angivna längden ingår i straffskalan för det brott som ingripandet gäller. Det innebär ett krav på att åtminstone det i straffskalan angivna maximistraffet ska nå den nivån (jfr t.ex. 24 kap. 1 § RB). Med en sådan utformning omfattar tillämpningsområdet i princip samtliga i det här sammanhanget relevanta brott. Sådana brott som inte är relevanta här och som endast kan föranleda böter kommer däremot att ligga utanför tillämpningsområdet. Att begränsa ingripandena på det sättet säkerställer att det nya verktyget bara får användas när det finns starka skäl för det, samtidigt som det ger Polismyndigheten, Säkerhetspolisen och Tullverket rimliga förutsättningar för att ingripa mot brott. Intresset av ett generellt och lättillämpat regelverk talar i samma riktning.

Med hänsyn till att ingripanden, förutom radering, får göras för att störa eller avbryta brottslig verksamhet i cybermiljö, behöver avgränsningen av tillämpningsområdet även anpassas till att ingripanden görs utan anknytning till ett konkret brott. När det gäller preventiva tvångsmedel begränsas tillämpningsområdet på så sätt att det anges att den brottsliga verksamheten ska innefatta brott av viss svårhetsgrad eller vissa särskilt angivna brott.

I det här fallet bör den utformning som används för att avgränsa tillämpningsområdet för preventiva tvångsmedel inte orsaka några tillämpningsproblem. Endast om det rör sig om situationer där viss brottslig verksamhet bedöms bestå i ett antal ringa brott, kan det innebära att den inte uppfyller kravet på tillräcklig svårhetsgrad.

Det är viktigt att säkerställa att brotten har koppling till cybermiljö. Det bör komma till uttryck i lagtexten genom ett krav på att brotten eller den brottsliga verksamheten begås eller kommer att begås i cybermiljö med hjälp av ett informationssystem.

Sammanfattningsvis anser utredningen att tillämpningsområdet bör begränsas till brott för vilket det är föreskrivet fängelse i ett år eller mer, eller brottslig verksamhet som innefattar sådant brott, och som begås eller kommer att begås i cybermiljö med hjälp av informationssystem.

14.7 Ingripandena ska vara proportionerliga

Utredningens förslag

Ett ingripande enligt lagen får göras endast om skälen för åtgärden uppväger det intrång eller men i övrigt som det innebär för den vars uppgifter blir föremål för ingripande eller för något annat motstående intresse.

Skälen för utredningens förslag

Allmänt om proportionalitetsprincipen

Som framgått av avsnitt 3.2 får skyddet gentemot det allmänna mot betydande intrång i den personliga integriteten enligt 2 kap. 6 § RF begränsas genom lag, men bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ RF). Genom 2 kap. 21 § RF uttrycks proportionalitetsprincipen vid lagstiftning. Regleringen i 8 § polislagen och 2 kap. 2 § tullbefogenhetslagen ger uttryck för bl.a. proportionalitetsprincipen när en tjänsteuppgift ska verkställas.

Proportionalitetsprincipen innebär att en åtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till motstående intressen. Det innebär att beslutsfattaren alltid måste beakta principen vid ett beslut om ingripande. Först ska dock beslutsfattaren pröva om ingripandet är tillåtet inom ramen för ändamålet. Därefter ska beslutsfattaren pröva om ingripandet faktiskt behövs och slutligen om ingripandet också är proportionerligt.

En viktig aspekt när det gäller proportionalitetsbedömningar är de hänsyn som ska tas till tryck- och yttrandefrihetslagstiftningen. Det är en fråga som, beroende på vilken typ av informationssystem som ett ingripande riktas mot, måste vägas in.

Tillämpningen på andra åtgärder än radering

Proportionalitetsprincipen innebär att skälen som talar för ett ingripande ska vägas mot det intrång eller men som ingripandet innebär. Om ingripandet kan förväntas medföra allvarlig skada på ett informationssystem kan avvägningen leda till att någon annan åtgärd bör användas, eller till att beslutsfattaren bör avstå från ingripande.

Proportionalitetsprincipen får betydelse för hur ett beslut bör utformas och vilka eventuella villkor som bör ställas. Den gäller vidare under hela genomförandet och ska alltså, även sedan beslut har fattats, beaktas självmant av den ingripande myndigheten. Det kan t.ex. uppstå en situation där integritetsintrånget under verkställigheten blir så stort att ingripandet inte längre kan anses vara proportionerligt, trots att ändamålet fortfarande är relevant och behovet av ingripande kvarstår.

Allvaret i det brott eller den brottsliga verksamhet som ligger till grund för ingripandet är av stor betydelse för bedömningen av om skälen för ingripandet uppväger det intrång eller men i övrigt som ingripandet innebär för den vars uppgifter blir föremål för ingripande eller något annat motstående intresse. Av vikt är också hur stort intrång i den personliga integriteten för utomstående eller hur stor skada eller annat men som brottet eller den brottsliga verksamheten i fråga kan komma att orsaka samhället eller enskilda om något ingripande inte görs.

Den minst ingripande åtgärden ska som utgångspunkt användas. Bara om någon annan åtgärd inte är tillräcklig för att uppnå den avsedda effekten, eller tekniskt eller praktiskt inte är möjlig att genomföra, får mer ingripande åtgärder användas. Styrkan i ett ingripande får som utgångspunkt avgöras utifrån det integritetsintrång eller men i övrigt som åtgärden innebär för enskilda vilkas uppgifter är föremål för ingripande. I den bedömningen ligger att hänsyn ska tas till karaktären av dels de uppgifter som ingripandet riktar sig mot, dels det informationssystem, eller delar av informationssystem, som ingripandet riktar sig mot.

Det är enligt utredningens mening stor skillnad om ingripandet riktas mot delar av digitala plattformar och tjänster, där det bedrivs normal verksamhet, eller om det är fråga om ett ingripande mot en del av ett informationssystem som understödjer brottslig verksam-

het eller har brott som enda ändamål. I de senare fallen väger samhällsintressena mycket tungt i förhållande till motstående intressen.

Tillämpningen på radering

För att radering ska vara tillåten krävs, till skillnad från övriga åtgärder, att ingripandet är av synnerlig vikt för att förhindra att brott begås eller för att avbryta brott i cybermiljö. Redan genom det kravet kommer det till uttryck att radering bör användas restriktivt. Radering bör komma i fråga först om andra mindre ingripande åtgärder, t.ex. blockering, har uttömts eller är otillräckliga för att uppnå syftet med ingripandet eller tekniskt eller praktiskt inte är möjliga att genomföra.

Med hänsyn till raderingens ingripande karaktär, bör den vidare endast komma i fråga om vissa typer av uppgifter. Som framgått av avsnitt 14.5.2, kan det röra sig om att planer på terroristbrott kan förhindras genom att terrorisminnehåll raderas eller att säkerhetskänslig information raderas för att förhindra eller avbryta spionerі eller olovlig underrättelseverksamhet. Det kan vidare röra sig om barnpornografimaterial som raderas för att förhindra spridning av materialet. Radering kan även avse en skadlig kod som raderas för att förhindra eller avbryta pågående brott mot människors liv och hälsa eller egendom.

När det gäller radering ställs inte sällan olika enskilda intressen mot varandra. Generellt kan sägas att avvägningen mellan exempelvis gärningsmannens intresse av att behålla pornografiskt, förnedrande eller på annat sätt integritetskränkande material och brottsoffers intresse av att det förstörs i de flesta fall framstår som självklar. Även avvägningen mellan den enskildes och samhällets intresse är i många fall enkel. Det gäller t.ex. i de fall där gärningsmannens intresse av att få behålla material som uppmuntrar till terroristbrott ställs mot samhällets intresse av att det inte sprids.

Avgörande för om åtgärden bör få vidtas bör vara hur stor skada som brottet eller den brottsliga verksamheten kan orsaka samhället eller enskilda om uppgifterna inte raderas. Finns det risk för att brottsligheten kan drabba t.ex. människors liv eller hälsa eller utgöra ett hot mot rikets säkerhet kan radering oftare vara proportionerlig än vid brottslighet som främst drabbar ekonomiska intressen. Om

exempelvis planer på terroristbrott kan avvärjas eller förlust av säkerhetskänslig information kan förhindras väger det tyngre än t.ex. att romansbedrägerier kan förhindras. Om en mängd otillåtet åtkomna personuppgifter påträffas i ett dokument eller en fil i en persons dator och det finns risk för att uppgifterna sprids i illegitimt syfte, kan radering av personuppgifterna vara mycket viktig för de personer vilkas personuppgifter det rör sig om. Det kan vidare vara nödvändigt att radera t.ex. en skadlig kod som kan orsaka stor skada för samhällsviktig verksamhet.

Det finns också skäl att skilja mellan radering av enstaka filer, bilder eller dokument och radering av många uppgifter i ett informationssystem. Det senare kräver att skälen för radering är mycket starka.

Nedstängning av hela digitala plattformar är sällan proportionerligt

Utredningen ställer sig mycket tveksam till att de brottsbekämpande myndigheterna ska tillåtas att stänga ner hela webbplatser. En sådan åtgärd aktualiserar svåra gränsdragningar i förhållande till annan lagstiftning, inte minst grundlagsfrågor om yttrandefrihet. Att stänga ner hela digitala plattformar i form av t.ex. sociala medier, Sveriges Radios webbplats eller någon annan digital plattform som används av ett mycket stort antal personer och företag kan knappast under några omständigheter anses vara proportionerligt, oavsett hur allvarligt brott det kan vara fråga om. Allmänhetens intresse av att digitala plattformar av det slaget inte stängs ner och det ekonomiska avbräck som en sådan åtgärd skulle kunna leda till gör det oproportionerligt. Att stänga ner en hel digital plattform skulle dels stå i strid med utgångspunkten att ingripandena ska riktas mot uppgifter i informationssystemen och skulle dessutom i de allra flesta fall även av andra skäl vara en alltför ingripande åtgärd. Det torde inte heller vara proportionerligt att stänga ner en myndighets eller ett större företags webbplats på grund av att t.ex. en anställd begår brott med hjälp av webbplatsen.

Däremot kan det, som tidigare nämnts, beroende på omständigheterna i det enskilda fallet, vara proportionerligt att stänga ner en viss digital plattform som har ett tydligt illegitimt syfte. Det kan vara nödvändigt för att få kontroll över den verksamhet som bedrivs på

plattformen. Mer begränsade åtgärder, t.ex. att stänga ett visst användarkonto på en kommunikations- eller lagringstjänst, torde ofta kunna anses proportionerligt.

14.8 Åtgärdernas koppling till ändamålet

Ett ingripande förutsätter att den ingripande myndigheten har behov av att vidta åtgärden. I de allra flesta fall innebär det ett behov av att bereda sig tillgång till ett informationssystem och till uppgifter i det, i syfte att kunna vidta en specifik åtgärd, om det inte kan göras på något mindre ingripande sätt. Det kan dock inte uteslutas att vissa hindrande åtgärder kan vidtas utan att myndigheten först bereder sig tillgång till informationssystemet.

Varje åtgärd bör ha en tydlig koppling till ändamålet med ingripandet. Det måste lämnas utrymme för den ingripande myndigheten att på det minst skadliga sättet bereda sig tillgång till uppgifterna i fråga. De åtgärder som därefter vidtas får emellertid endast vidtas i den eller de delar av informationssystemet som har samband med brott eller brottslig verksamhet av tillräcklig svårhetsgrad och ska syfta till att förhindra eller avbryta brottet eller störa eller avbryta den brottsliga verksamheten. Det kan t.ex. vara fråga om att en ingripande myndighet ändrar ett lösenord så att den person som äger eller använder informationssystemet utesluts från tillgång till det, vilket förhindrar personen från att begå bedrägeri via en digital plattform. Det kan också vara fråga om att tillgången till en webbplats blockeras, för att förhindra försäljning av illegala varor.

Det sagda gäller även ingripanden för att kartlägga kommunikation mellan informationssystem. Den åtgärden har enbart till syfte att kartlägga om det förekommer kommunikation till och från informationssystem som kan antas utnyttjas i brottslig verksamhet.

Även radering av uppgifter som behandlas i ett informationssystem måste ha koppling till ändamålet med ingripandet. Ett beslut om radering bör därför endast få avse specificerade uppgifter, t.ex. vissa bilder, viss information eller en viss programvara, som har tydligt samband med brott av tillräcklig svårhetsgrad. Syftet med raderingen ska vara att förhindra eller avbryta brott i cybermiljö.

Om ett ingripande görs för flera ändamål ska ändamålet med varje åtgärd vara uppfyllt.

Det som har sagts om kopplingen till ändamålet gäller även i de fall där ett nytt beslut om ingripande fattas, vilket framför allt kommer att aktualiseras vid blockering. Ett nytt beslut syftar då till att upprätthålla ändamålet.

15 Förbud mot ingripanden

15.1 Skyddet för viss verksamhet

Utredningens bedömning

Vissa informationssystem och uppgifter bör ha särskilt skydd mot ingripanden.

Skälen för utredningens bedömning

Viss information och verksamhet har ett starkare skydd

Information som hanteras för journalistiska ändamål, som har anförtrotts vissa yrkeskategorier i deras yrkesutövning eller som präster eller vissa andra religiösa företrädare fått veta vid själavård eller bikt har ett extra starkt skydd vid brottsutredning och lagföring. Regleringen knyts till undantagen från vittnesplikten i 36 kap. 5 § andra–sjätte styckena RB. Ända sedan RB infördes gäller enligt 27 kap. 2 § RB förbud mot att ta en skriftlig handling i beslag om den kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om, och handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för. Uppgifter av det slaget får inte heller avlyssnas vid hemlig avlyssning av elektronisk kommunikation eller hemlig rumsavlyssning (27 kap. 22 § RB). Vidare får ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning inte avse en plats som stadigvarande används eller är särskilt avsedd att användas för journalistiska ändamål eller som stadigvarande används eller är särskild avsedd att användas av någon av de tidigare nämnda yrkeskategorierna (27 kap. 22 a § RB). Motsvarande begränsningar gäller vid hemlig dataavläsning av informationssystem som stadigvarande används i de

verksamheter och av de yrkeskategorier som har nämnts (11 och 27 §§ lagen om hemlig dataavläsning).

Regleringen innebär inte bara ett förbud mot att ge tillstånd till hemliga tvångsmedel som avser sådan information som har särskilt skydd. Förbuden riktar sig också till verkställande myndigheter för att de – om det skulle visa sig att sådana uppgifter som inte är tillåtna att hämta in oavsiktligt ändå har inhämtats – omedelbart ska kunna avbryta pågående verkställighet eller granskning och förstöra det material som omfattas av förbuden.

Motsvarande skydd bör gälla enligt den nya lagen

Om ingripanden i cybermiljö ska tillåtas måste regleringen enligt utredningens mening utformas på sådant sätt att särskilt integritetskänslig information så långt möjligt skyddas, utan att det går ut över effektiviteten i åtgärderna. Det är inte tillräckligt att frågan om beslut om ingripande ska fattas kan beaktas inom ramen för proportionalitetsbedömningen, eftersom ingripandet kan komma att omfatta särskilt integritetskänslig information. I informationssystem som används av bl.a. journalister, advokater, läkare och präster finns det normalt en mängd känsliga uppgifter som är så skyddsvärda att sekretessen för dem bör få företräde framför det brottsbekämpande intresset. Det behövs därför ett starkt skydd, så att sådana uppgifter varken kan avslöjas eller spridas vidare till obehöriga. Ett ingripande enligt lagen bör därför inte få avse sådan verksamhet eller sådana uppgifter som anses vara särskilt skyddsvärda (jfr Hemlig rumsavlyssning, prop. 2005/06:178, s. 62 och prop. 2019/20:64 s. 137).

15.2 Utformningen av förbudet

Utredningens förslag

Ett ingripande enligt den nya lagen får inte avse ett informationssystem som stadigvarande används eller är särskilt avsett att användas i verksamhet

1. där tystnadsplikt gäller enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL, eller

2. för bikt eller enskild själavård som bedrivs av präster inom trossamfund, eller av dem som har motsvarande ställning inom sådana samfund.

En åtgärd får inte heller avse sådana uppgifter i ett informationssystem som någon, på grund av bestämmelser i 36 kap. 5 § andra och tredje styckena RB, inte skulle ha kunnat höras som vittne om.

Om den ingripande myndigheten får kännedom om att det är fråga om sådana informationssystem eller sådana uppgifter som omfattas av förbud ska ingripandet omedelbart avbrytas och eventuell information som myndigheten har fått tillgång till ska förstöras i den del det omfattas av förbud.

Skälen för utredningens förslag

Utgångspunkter för regleringen

Regleringen i 36 kap. 5 § andra–sjätte styckena RB har tillkommit av hänsyn till enskildas personliga integritet, för att skydda deras privatliv. Lagstiftaren har ansett att den enskilde, förutom när det är fråga om mycket allvarliga brott, och i vissa fall även då, ska kunna anförtro sig till vissa yrkeskategorier utan rädsla för att samtalet eller de uppgifter som han eller hon lämnar ska komma till tredje mans kännedom eller annars användas emot honom eller henne (prop. 2005/06:178 s. 63).

I 36 kap. 5 § andra stycket RB föreskrivs att personer som tillhör vissa yrkeskategorier vid en rättegång inte får tillfrågas om sådant som de har anförtrotts i deras yrkesutövning eller som de erfarit i samband med den. De yrkeskategorier som avses är bl.a. advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter, familjerådgivare enligt socialtjänstlagen (2025:400) och deras biträden.

I 36 kap. 5 § tredje stycket RB föreskrivs att rättegångsombud, biträden och försvarare, oavsett om de är advokater eller inte, inte får höras som vittne om det som de har anförtrotts för att fullgöra uppdraget.

De som tillhör de tidigare angivna yrkeskategorierna är dock, trots sin tystnadsplikt, enligt 36 kap. 5 § fjärde stycket RB skyldiga

att vittna i mål om allvarliga brott. Det sagda gäller dock inte försvarare. Vittnesplikten gäller också om den till vars förmån tystnadsplikten gäller medger att personen hörs.

Enligt 36 kap. 5 § femte stycket RB får den som är präst inom ett trossamfund, eller den som i ett sådant samfund har motsvarande ställning, inte höras som vittne om något som han eller hon har erfarit under bikt eller enskild själavård. Från den bestämmelsen finns det inga undantag. Det innebär att präster och andra med liknande ställning aldrig får höras som vittnen om vad de erfarit i de situationerna.

Enligt 36 kap. 5 § sjätte stycket RB får den som har tystnadsplikt enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL höras som vittne om förhållanden som tystnadsplikten avser endast i den mån det föreskrivs i 3 kap. 4 § TF eller 2 kap. 4 § YGL.

Begränsningarna i skyldigheten att vittna gäller enligt 36 kap. 5 § sjunde stycket RB även den som biträtt med tolkning eller översättning.

Det ligger enligt utredningens mening nära till hands, att jämföra ingripanden i cybermiljö med den reglering som begränsar möjligheterna att använda vissa tvångsmedel. Skyddsintressena är likartade. En viktig skillnad är emellertid att syftet med åtgärderna skiljer sig åt. Syftet med att använda tvångsmedel i en förundersökning är att hämta in information som kan användas för brottsutredning och lagföring. Även i de fall där tvångsmedel används i underrättelseverksamhet är syftet att samla in information, vilket ofta i förlängningen leder till brottsutredning, även om det primära syftet är att förhindra brott.

Eftersom den nya lagen enbart reglerar ingripanden i syfte att hindra, avbryta eller störa brott och brottslighet i cybermiljö, inte att hämta in, bearbeta och lagra information är risken för att myndigheterna ska få tillgång till sådant som omfattas av förbud betydligt mindre än vid användning av tvångsmedel. Det bör emellertid ändå införas förbud mot att ta del av och behålla sådant som myndigheterna oavsiktligt kan ha fått tillgång till.

Förbudet bör endast avse vissa informationssystem

Tystnadsplikten enligt 3 kap. 3 § TF och 2 kap. 3 § YGL är ett centralt inslag i rätten för den som lämnar information för publicering att vara anonym. Bestämmelserna om undantag från tystnadsplikten är uttömmande. De infördes bl.a. mot bakgrund av det vitala samhällsintresset av att mycket grova brott mot rikets säkerhet kan upptäckas (proposition om ändringar i grundlagsregleringen av tryckfriheten, prop. 1975/76:204, s. 142). Även om tystnadsplikten inte är absolut, eftersom den inte gäller vid ett fåtal mycket allvarliga brott, är skyddet mycket starkt. Förbudet enligt den nya lagen bör enligt utredningens mening korrespondera med tystnadsplikten enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL.

Den tystnadsplikt som gäller enligt 36 kap. 5 § femte stycket RB är absolut för den som är präst inom ett trossamfund eller den som i ett sådant samfund har motsvarande ställning när det gäller något som han eller hon har fått veta under bikt eller enskild själavård. Förbudet enligt den nya lagen bör därför korrespondera med regleringen i 36 kap. 5 § femte stycket RB.

Det bör föreskrivas att förbudet mot ingripanden enbart ska avse sådana informationssystem som stadigvarande används eller är avsedda att användas i sådan verksamhet som avses i 36 kap. 5 § femte och sjätte styckena RB. Syftet är alltså inte att skydda informationssystem mot ingripanden bara därför att de ägs eller används av någon som bedriver i och för sig skyddad verksamhet. Det innebär att t.ex. besöksdatorer i en skyddad verksamhet, som inte kan sägas användas i ett sådant syfte som förbudet tar sikte på, inte omfattas av förbudet. Kravet på stadigvarande användning innebär att informationssystem som enbart tillfälligt används för de angivna syftena inte heller har det särskilda skyddet.

Frågan om ett informationssystem som används utanför en tidningsredaktion ska omfattas av motsvarande förbud behandlades när bestämmelserna om hemlig avlyssning av elektronisk kommunikation ändrades så att skyddet mot avlyssning stärktes. Lagrådet påpekade att begreppet stadigvarande användning inte behöver vara begränsad till att avse ett medieföretags redaktion utan också kan omfatta t.ex. en arbetsplats i en journalists hem. Regeringen instämde i det (Hemliga tvångsmedel mot allvarliga brott, prop. 2013/14:237, s. 180 och 297). Motsvarande gäller vid hemlig dataavläsning. Samma

synsätt bör enligt utredningens mening gälla i fråga om ingripanden i cybermiljö. Den fysiska arbetsplatsen är således inte avgörande för om informationssystemet kan bli föremål för ett ingripande. Det saknar betydelse om informationssystemet befinner sig på eller utanför arbetsplatsen. Det avgörande är om informationssystemet stadigvarande används för vissa fredade verksamheter (jfr prop. 2019/20:64 s. 138). Det innebär t.ex. att en dator eller mobiltelefon, som stadigvarande används för skyddad verksamhet, i vissa fall kan vara oåtkomlig för de brottsbekämpande myndigheterna. Ett exempel kan vara en präst som förvarar barnpornografi i sin tjänstemobil. Det är en sedan länge accepterad effekt av att viss information har ett starkare skydd.

Förbudet mot ingripanden mot informationssystem som används i verksamhet för bikt eller enskild själavård, som bedrivs av präster eller av dem som har motsvarande ställning inom trossamfund, bör omfatta informationssystem som används i verksamhet som bedrivs i t.ex. kyrkor, synagogor och moskéer. Förbudet bör emellertid inte gälla enbart därför att ett informationssystem används på en sådan plats. Det ska vara fråga om informationssystem som stadigvarande används eller är särskilt avsedda att användas i verksamhet för bikt eller själavård. Det är alltså inte platsen som sådan som är fredad från ingripanden utan systemen. Ytterst blir det en fråga vid tillståndsprövningen och verkställigheten i varje enskilt fall att bedöma om ett beslut om ingripande kan genomföras (jfr prop. 2019/20:64 s. 139).

Sammanfattningsvis innebär förslaget att ett ingripande inte får avse informationssystem som stadigvarande används eller är särskilt avsedda att användas dels i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL, dels i verksamhet för bikt eller enskild själavård som bedrivs av präster eller av dem som har motsvarande ställning inom trossamfund. När det gäller tystnadsplikten enligt TF och YGL kan den brytas, om den till vars förmån tystnadsplikten gäller medger det. I de fallen finns det inget som hindrar att ett ingripande görs, så länge det inte inkräktar på tystnadsplikt till förmån för någon annan.

Förbudet bör även avse vissa uppgifter i informationssystem

Det finns skäl att även skydda vissa andra särskilt skyddsvärda uppgifter från ingripanden enligt den nya lagen. Det rör sig om uppgifter som har anförtrotts sådana yrkeskategorier som advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen och rättegångsombud, deras biträden och försvarare som inte är advokater i deras yrkesutövning eller som de har erfarit i samband med den. När det gäller de yrkeskategorierna är skyddet – med undantag av det som gäller för försvarare – inte lika starkt, men liknande hänsyn bör tas. Det är viktigt att den som anförtror sig till sådana yrkeskategorier kan förlita sig på deras tystnadsplikt.

Det har i olika lagstiftningsärenden diskuterats i vilken utsträckning lokaler och informationssystem som används av bl.a. advokater, läkare, psykologer och andra yrkeskategorier som anges i 36 kap. 5 § andra och tredje styckena RB bör skyddas mot användning av hemliga tvångsmedel (se bl.a. Lagrådets och regeringens synpunkter i prop. 2005/06:178 s. 66 och 199). Ett förbud i nu aktuellt avseende skulle enligt utredningens mening kunna utformas så att förbudet tar sikte på uppgifter som har anförtrotts yrkeskategorierna i fråga i deras yrkesutövning och som finns i informationssystem. Ingripanden bör alltså inte få avse uppgifter som någon som, på grund av bestämmelserna i 36 kap. 5 § andra och tredje styckena RB, inte skulle ha kunnat höras som vittne om.

Det är i och för sig inget som hindrar att en brottsbekämpande myndighet bereder sig tillgång till ett informationssystem som används av någon i de skyddade yrkeskategorierna, under förutsättning att ingripandet inte avser uppgifter som denne har anförtrotts i sin yrkesutövning och som han eller hon inte får höras som vittne om. Skyddet avser uppgifter i informationssystem som används, privat eller i tjänsten, av någon av de nämnda yrkeskategorierna och som innehåller uppgifter som inte får röjas på grund av tystnadsplikten. Det avgörande är alltså inte hur eller av vem informationssystemet används utan uppgifterna som sådana. Det bör framhållas att den till vars förmån tystnadsplikten gäller kan lämna sitt medgivande till att den bryts. I de fallen finns det inget som hindrar att ett ingripande görs, så länge det inte inkräktar på tystnadsplikt till förmån för någon annan.

Skyldigheten att agera om förbjuden information upptäcks

I de fall där det vid användning av hemliga tvångsmedel gäller förbud mot att avlyssna eller avläsa viss information, föreskrivs skyldighet för den verkställande myndigheten att omedelbart avbryta verkställigheten, om det kommer fram att det är fråga om sådana uppgifter, och att omedelbart förstöra det material som har inhämtats och som omfattas av förbudet (27 kap. 22 § RB, 11 § lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott [preventivlagen] och 27 § lagen om hemlig dataavläsning). Vid granskning i efterhand av material från sådana tvångsmedel är det i stället granskningen som omedelbart ska avbrytas. Skälet till det är, enligt förarbetena till ändringar i lagen om hemlig dataavläsning, att det kan vara svårt, och ofta omöjligt, för myndigheterna att vid själva inhämtningen av materialet avgöra om det är fråga om uppgifter som omfattas av förbud. Då är det granskningen av materialet, inte verkställigheten, som bör avbrytas (se prop. 2024/25:51 s. 59 f.). Förstöringskravet är detsamma oavsett när det upptäcks att det är fråga om uppgifter som omfattas av förbud.

När det gäller ingripanden i cybermiljö torde det i praktiken i de flesta fall vara först när de ingripande myndigheterna har berett sig tillgång till ett informationssystem och tar del av uppgifter i det som de kan upptäcka om de uppgifter som är föremål för ingripande omfattas av förbud. En liknande reglering som den som gäller för vissa tvångsmedel bör därför införas för ingripanden i cybermiljö. Det behövs för att säkerställa att den brottsbekämpande myndigheten omedelbart avbryter ingripandet i den del det omfattas av förbud.

Som framgått av avsnitt 14.2 medger inte den nya lagen att myndigheterna hämtar in uppgifter genom att t.ex. kopiera dem eller på annat sätt föra över dem till egna informationssystem som är fallet vid hemlig dataavläsning. Om det ändå skulle göras, t.ex. på grund av ett misstag från myndighetens sida, bör det ställas krav på att eventuell information som myndigheten har fått tillgång till och som omfattas av förbud ska förstöras omedelbart. Minnesanteckningar eller liknande som myndigheten för i samband med ingripandet bör emellertid inte omfattas av förbudet, så länge de inte återger uppgifter som myndigheten är förbjuden att ta del av.

Som utredningen återkommer till i avsnitt 20.1.2 kan ingripanden i cybermiljö i ett antal fall antas utmynna i att brott upptäcks och

blir föremål för förundersökning. Frågan hur sådant som blir tillgängligt för brottsbekämpande myndigheter vid ett ingripande i cybermiljö ska hanteras kommer att diskuteras närmare där.

Finns det risk för att skyddsreglerna missbrukas?

De brottsbekämpande myndigheterna har framhållit att både främmande makt och kriminella anpassar sig till lagstiftningen och aktivt utnyttjar undantag och skyddsregler i lagstiftningen i sin verksamhet. Det innebär att de kan komma att utnyttja det förhållandet att starkare skyddsregler gäller för vissa verksamheter eller vissa informationssystem, t.ex. genom att – i det fördolda – utnyttja sådana informationssystem eller att placera informationssystem på platser som är fredade mot intrång. Brottsbekämpningen kan enligt myndigheterna bli lidande om det är enkelt att kringgå lagstiftningen.

Utredningen har förståelse för de farhågor som myndigheterna har framfört. Det finns framför allt vissa risker som kan hänföras till att den teknik som används inte är tillräckligt motståndskraftig mot angrepp eller till att de personer som arbetar i verksamheterna i fråga inte är tillräckligt uppmärksamma på riskerna. Mot de riskerna ska ställas det intrång i den personliga integriteten som det innebär att myndigheter skaffar sig tillgång till informationssystem och uppgifter som behandlas i dem. I dagens digitaliserade samhälle innehåller enskildas informationssystem betydligt fler och mer integritetskänsliga uppgifter än tidigare, bl.a. till följd av de närmast obegränsade lagringsmöjligheterna. Det är således två, var för sig viktiga, men motstridiga intressen som ställs mot varandra. Enligt utredningens mening är den föreslagna lösningen en rimlig avvägning mellan de intressena. Den ligger dessutom väl i linje med hur intressena har vägts mot varandra i andra sammanhang.

16 Vem som bör besluta om ingripanden

16.1 Polismyndigheten, Säkerhetspolisen och Tullverket bör besluta om flertalet åtgärder

Utredningens förslag

Särskilt utsedda befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket får besluta om alla typer av ingripanden utom radering. De får då även besluta om tillträde.

Skälen för utredningens förslag

Åtgärdernas karaktär bör avgöra vem som får besluta

Syftet med den nya regleringen är, som tidigare har nämnts, att skapa förutsättningar för att brottsbekämpande myndigheter så tidigt som möjligt ska kunna ingripa mot brott i cybermiljö och att ge de brottsbekämpande myndigheterna förutsättningar att kunna fullgöra sitt uppdrag även i cybermiljö. På samma sätt som vid ingripanden i den fysiska miljön kan det därmed inte krävas att det råder visshet om att ett brott har begåtts eller har påbörjats innan ingripandet görs. Tvärtom finns mycket att vinna med att kunna störa brottslig verksamhet och hindra att brott kan sättas i verket eller att i vart fall avbryta pågående brott. Det ställs inget krav på att beslut om ingripanden bara ska få fattas inom ramen för förundersökning eller att det ska förekomma underrättelseverksamhet inriktad på den aktuella brottsligheten. Ett ingripande kan t.ex. föregås av informationsinsamling om ett visst fenomen som misstänks vara brottsligt eller av en anmälan från en enskild. Det kan också föranledas av tips från

allmänheten, en myndighet eller ett utländskt brottsbekämpande organ. Det sagda talar för att beslut om ingripanden i cybermiljö, på samma sätt som ingripanden i den fysiska miljön, bör fattas av den myndighet som har till uppgift att ingripa mot företeelsen i fråga. Det finns dock anledning att gå närmare in på vilka skäl som talar för de tänkbara alternativen, vilka är att beslut om ingripanden fattas av domstol, av åklagare eller av polisen respektive Tullverket.

Beslut av domstol?

Det kan hävdas att ingripanden som riktar sig mot informationssystem generellt är så integritetskänsliga att de bör jämställas med beslut om hemliga och preventiva tvångsmedel och därmed kräva samma typ av kvalificerad beslutsfattare. Det rör sig visserligen om sådana ingrepp i privatlivet som faller under artikel 8 i Europakonventionen, men det innebär bara att det krävs en tydlig och förutsebar lagreglering, inte att det ställs krav på en viss typ av beslutsfattare. Som exempel kan nämnas att en husrannsakan i ett enskilt fall kan innebära ett minst lika stort intrång i den enskildes privatliv som ett hemligt tvångsmedel, men det ställs inte något generellt krav på en särskilt kvalificerad beslutsfattare för husrannsakan.

Som tidigare nämnts kan det förhållandet att ingripandena ska göras i cybermiljö och riktar sig mot informationssystem inte automatiskt innebära att de kan jämföras med andra typer av åtgärder som får vidtas med informationssystem. Det är enligt utredningens mening en betydande skillnad mellan de ingripanden som kan bli följden av den föreslagna nya lagen och användningen av hemliga tvångsmedel. Tvångsmedlen i fråga syftar till att i hemlighet hämta in, analysera och bearbeta information som kan läggas till grund för brottsutredning och lagföring. Tvångsmedlen används under längre tid, på ett systematiskt och på förväg planerat sätt med ett tydligt mål. Ett ingripande enligt den nya lagen är avsett att vara kortvarigt och i första hand syfta till att stoppa eventuell brottslig verksamhet och förhindra framtida brott. I många fall görs därför ingripandet öppet. Här bortses från att det i vissa fall kan ta lång tid att förbereda själva ingripandet, t.ex. om det förutsätter att ett beslut om tillträde utnyttjas eller att systemskydd behöver brytas eller kringgås.

Det sannolika är att det, när ingripanden enligt den nya lagen aktualiseras, i många fall inte finns någon förundersökning om konkreta brott och kanske inte heller någon pågående underrättelseverksamhet som är inriktad på den aktuella brottsligheten. Om det förekommer underrättelseverksamhet är det troligt att den riktar sig mot ett visst fenomen, inte mot en viss person eller ett specifikt informationssystem. Det kan röra sig om såväl systematiska bedrägerier, utpressning eller sexualbrott mot barn som angrepp från främmande makt i form av spionerі eller andra brott som riktar sig mot Sveriges säkerhet. Ett brottsligt fenomen, där det i princip saknas kunskap om de allra flesta detaljer som kan vara avgörande för om det finns rättslig grund för att inleda förundersökning, eller att använda preventiva tvångsmedel, ligger långt ifrån den nivå där domstolsbeslut normalt fattas.

Även om effekterna av ett ingripande i cybermiljö i vissa fall kan förväntas bli så stora att det talar för att beslut enligt den nya lagen bör fattas av domstol, finns det dock flera skäl som talar mot att domstol bör fatta besluten i fråga.

Det är nämligen inte ens alla typer av hemliga tvångsmedel som i dag kräver domstolsbeslut. Beslut om inhämtning enligt inhämtningslagen fattas i de flesta fall av åklagare efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket. Det enda undantaget är motsvarande inhämtning som görs genom hemlig dataavläsning, där det krävs beslut av domstol. Tidigare fattade Polismyndigheten, Säkerhetspolisen och Tullverket själva beslut om inhämtning.

Samma argument som ansetts tala mot att beslut fattas av domstol i inhämtningsärenden (prop. 2011/12:55 s. 88 f.), framför allt att det skulle vara en främmande roll för domstolarna, kan anföras när det gäller ingripanden enligt den nya lagen. Det underlag som finns när ingripandet aktualiseras är normalt underrättelseuppgifter, som kan vara fragmentariska, motsägelsefulla och svåra att värdera utan ingående kunskaper om hur underrättelseverksamhet bedrivs. Polisiära ingripanden är en typiskt operativ uppgift, vars utfall är svårt att förutsäga och som kan behöva anpassas successivt, beroende på det som kommer fram under ingripandet. Till det kommer att det i många fall kan behövas mycket snabba beslut, om ett ingripande ska bli framgångsrikt. Domstolarna har i dag inte samma förutsättningar som åklagare, polisen och Tullverket har att kunna hantera snabbt beslutsfattande.

Sammanfattningsvis anser utredningen därför att domstol inte bör fatta beslut om ingripanden enligt den nya lagen.

Beslut av åklagare?

Det är, som framgått, av stor vikt att i vissa fall mycket snabbt kunna ingripa mot brott och brottslig verksamhet i cybermiljö. Snabbhet i förfarandet kommer enligt de brottsbekämpande myndigheterna att vara en avgörande faktor för att ingripandena ska bli framgångsrika. De som begår brott eller bedriver brottslig verksamhet med hjälp av informationssystem vidtar ofta aktivt åtgärder i syfte att försvåra brottsbekämpningen. Ofta är möjligheten till snabba beslut därför avgörande för att kunna ingripa. Beslut om ingripanden kan även, beroende på vad som kommer fram vid ingripandet, löpande behöva anpassas efter omständigheterna i det enskilda fallet.

Frågan är då om åklagare bör fatta beslut om ingripanden enligt den nya lagen. Det finns, genom systemet med jour och beredskap, i princip åklagare tillgängliga dygnet runt som skulle kunna fatta sådana beslut. Det skulle kunna kombineras med en ordning där de brottsbekämpande myndigheterna tillåts fatta intermistiska beslut i situationer där ingripandet är så brådskande att det inte är möjligt att avvakta ett beslut av åklagare.

Ett ingripande i cybermiljö kan, som nyss nämnts, röra brott på förundersökningsnivå, men även brott och brottslig verksamhet på underrättelsestadiet. Det kan i många avseenden jämföras med polisiära ingripanden i fysisk miljö, där det sällan på förhand går att avgöra vad ett ingripande kommer att resultera i. Även om åklagarnas kärnverksamhet är att leda förundersökningar och att processa i domstol, och de därmed normalt inte har någon uppgift i underrättelseverksamheten, finns det redan i dag vissa uppgifter i sådan verksamhet som ankommer på åklagare. Det rör sig främst om åklagarnas roll att fatta beslut enligt inhämtningslagen och att hantera tvångsmedel enligt preventivlagen. Beslut enligt framför allt preventivlagen anses ligga nära de beslut som åklagare fattar inom ramen för förundersökningsverksamhet (Datalagring vid brottsbekämpning – anpassningar till EU-rätten, prop. 2018/19:86, s. 73). Även beslut enligt inhämtningslagen har ansetts ligga tillräckligt nära åklagarnas normala verksamhet.

Det finns dock enligt utredningens mening skäl som talar mot att åklagare ska fatta beslut om ingripanden enligt den nya lagen.

Allmänna åklagares huvuduppdrag är att leda förundersökning och väcka åtal för brott som hör under allmänt åtal. Åklagarna tar, med de undantag som nyss nämnts, inte del i underrättelseverksamhet. Åklagare övertar normalt ledningen av en förundersökning först när den har inletts och någon är skäligen misstänkt för brottet. I fall som avser mycket allvarliga brott och i vissa andra situationer där det krävs en kvalificerad beslutsfattare övertar åklagaren ledningen av förundersökningen tidigare. Vidare förekommer det ibland samråd mellan Polismyndigheten, Säkerhetspolisen respektive Tullverket och åklagare i frågan om det finns tillräckliga skäl att inleda förundersökning eller om det krävs ytterligare underrättelse- eller spaningsåtgärder. Även om åklagare således i viss utsträckning kan vara delaktiga i underrättelseverksamhet är den uppgiften som regel begränsad till konkreta ärenden och situationer där en förundersökning är nära förestående.

Ingripanden i cybermiljö kommer i många fall att göras på ett betydligt tidigare stadium än när en förundersökning är nära förestående. Det kan förutsättas att det sällan finns någon anknytning till ett specifikt brott eller en pågående brottsutredning, även om så kan vara fallet i något undantagsfall. Det talar starkt mot att lägga beslutsbefogenheten på åklagare, även om åklagare i viss utsträckning kan vara delaktiga i underrättelseverksamhet. Om ett ingripande enligt den nya lagen skulle aktualiseras, samtidigt som det förekommer en åklagarledd förundersökning som berör samma fråga eller samma person, bör dock beslut om ingripande inte fattas innan samråd med åklagaren har ägt rum. Annars finns det risk att ingripandet stör eller försvårar den pågående förundersökningen. Det kan enligt utredningens mening lämpligen regleras i förordning.

Beslut av Polismyndigheten, Säkerhetspolisen eller Tullverket?

Det återstår då att överväga om Polismyndigheten, Säkerhetspolisen och Tullverket bör få besluta om ingripanden enligt den nya lagen. Ur kontrollsynpunkt kan det hävdas att beslut inte bör fattas av den myndighet som ska genomföra åtgärden. Så är emellertid fallet när det gäller många av de tvångsmedel och andra åtgärder som får an-

vändas i en förundersökning och som också kan vara mycket integritetskänsliga. Polismän och tulltjänstemän har sedan lång tid befogenhet att fatta beslut om bl.a. gripande, husrannsakan och beslag. Det förhållandet motsvarar regleringen i de flesta andra länder och är något som anses vara väl förenligt med Europakonventionen. Numera ställs det enligt 23 kap. 4 § RB samma krav på objektivitet i brottsbekämpande verksamhet före som under en förundersökning.

Beslut om brottsbekämpande åtgärder bör som utgångspunkt inte ligga på en högre nivå än vad som är sakligt motiverat. Att den nya lagen reglerar ingripanden på operativ nivå och att det kan krävas att beslut fattas mycket snabbt talar starkt för att beslut bör fattas av Polismyndigheten, Säkerhetspolisen respektive Tullverket. Europadomstolen ställer inte något krav på att domstol eller något annat oberoende organ ska fatta beslut om att ingripa mot brott på det sätt som nu är aktuellt. Enbart den omständigheten att ingripandena ska göras i cybermiljö motiverar enligt utredningens mening inte heller att beslut bör fattas på en högre nivå. Den nya lagen ger de brottsbekämpande myndigheterna rättsliga förutsättningar att fullgöra sina uppdrag i cybermiljön, även om tillämpningsområdet för lagen är snävare än för ingripanden i den fysiska miljön.

Om beslut om ingripanden får fattas av befattningshavare vid Polismyndigheten, Säkerhetspolisen respektive Tullverket bör det emellertid ställas särskilda krav på en sådan beslutsfattare. Det bör vara någon som dels har goda kunskaper om digitala informationssystem och informationssäkerhet, dels den särskilda kompetens, utbildning och erfarenhet som är nödvändig och även i övrigt är särskilt lämpad för uppdraget. Det bör vara fråga om av myndigheten särskilt utpekade befattningshavare. De närmare kraven kan regleras i förordning.

Det som nu har sagts om beslutsnivån bör gälla alla typer av ingripanden i cybermiljö som är av sådan natur att enskilda kan återfå rådigheten över informationssystem eller uppgifter som har varit föremål för ingripanden. När det gäller radering, som är en åtgärd av oåterkallelig karaktär, bör det dock ställas högre krav på beslutsfattare, vilket utredningen återkommer till.

Slutsatser

Sammanfattningsvis anser utredningen att varken allmän domstol eller åklagare bör fatta beslut om ingripanden enligt den nya lagen. I stället talar övervägande skäl för att särskilt utpekade befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket bör besluta om sådana åtgärder, så länge det inte är fråga om radering. Det innebär att beslut om att bereda sig tillgång till informationssystem och till uppgifter i det i syfte att ändra eller blockera uppgifter eller att genom någon annan liknande åtgärd störa eller hindra användningen av uppgifter som behandlas i informationssystem bör fattas av befattningshavare vid Polismyndigheten, Säkerhetspolisen respektive Tullverket. Detsamma gäller ingripanden för att klarlägga om det förekommer kommunikation till eller från ett informationssystem som kan antas utnyttjas i brottslig verksamhet. Utredningen återkommer till vad som bör gälla för beslut om radering.

De särskilt utpekade befattningshavarna bör även få besluta om tillträde enligt den nya lagen (se avsnitt 17.3).

16.2 Beslut om radering

16.2.1 Beslut om radering bör fattas av åklagare

Utredningens förslag

Åklagare får, på ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket, besluta om radering. Åklagaren får då även besluta om tillträde.

Skälen för utredningens förslag

Raderingsbeslut bör fattas av åklagare

Som framgått av avsnitt 14.5.2 kan radering av uppgifter i ett informationssystem vara en mer integritetskänslig åtgärd än andra typer av ingripanden i cybermiljö. Det är nämligen en åtgärd som är oåterkallelig. Det ligger därmed i sakens natur att radering kan orsaka större skada eller utgöra ett större integritetsintrång, än ett ingripande

som innebär att den enskilde kan återfå rådigheten över informationssystem eller uppgifter i systemet.

Det kan finnas situationer där radering innebär ett mindre integritetsintrång för den vars informationssystem blir föremål för ingripande än för den som har utsatts för det brott som ligger till grund för ingripandet. Så kan t.ex. vara fallet när det gäller övergreppsmaterial eller när personer har fått känsliga personuppgifter stulna. Sådana omständigheter, som kräver stor vana vid komplext beslutsfattande, ska beaktas inom ramen för proportionalitetsbedömningen vid beslutet (avsnitt 14.7).

Utredningen anser att det bör ställas högre krav på de omständigheter som får läggas till grund för radering än för andra ingripanden i cybermiljö. Därför föreslås att beslut om radering får fattas endast om det är av synnerlig vikt för att förhindra eller avbryta brott i cybermiljö. Utredningen anser vidare att det av rättssäkerhetsskäl bör ställas krav på en mer kvalificerad beslutsfattare. Om möjligt bör beslutsfattaren vara fristående från den ansökande myndigheten. En lämplig lösning kan vara att beslut om radering fattas av åklagare.

Ett viktigt skäl, som talar för att åklagare bör vara beslutsfattare, är att radering kan få negativa konsekvenser för eventuell framtida brottsutredning och lagföring av det brott som åtgärden avser. Den frågan avgörs bäst av åklagare.

Något som också bör vägas in när det gäller radering är att beslut om radering i många fall inte kommer att vara lika brådskande som andra ingripanden enligt lagen. Det finns flera skäl för det. Ett är att radering är en oåterkallelig åtgärd som förutsätter att ingripandet är av synnerlig vikt. Det innebär att det måste finnas ett fylligare underlag för bedömning innan beslut om radering kan fattas än för andra ingripanden enligt lagen. Vidare kan blockering ofta vara en lämpligare åtgärd än radering. Ett annat skäl är att radering som omfattar exempelvis barnpornografi eller övergreppsmaterial som regel kommer att avse material som redan har funnits på internet en längre tid. Radering är alltså i många fall inte något som behöver beslutas omedelbart.

Med hänsyn till det nyss sagda anser utredningen att övervägande skäl talar för att åklagare bör besluta om radering, utom i brådskande fall, vilket utredningen återkommer till. Åklagaren bör även kunna fatta beslut om tillträde, om det behövs för att kunna genomföra raderingen (se avsnitt 17.3).

En alternativ lösning?

Utredningen har även övervägt om särskilt utpekade befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket bör få besluta om radering av uppgifter i de fall där uppgifterna kan säkras genom en kopia. En sådan beslutsordning innebär enligt Polismyndigheten att raderingen i sådana fall inte skulle få samma negativa konsekvenser för den enskilde som radering annars kan få. Det är emellertid enligt utredningens mening viktigt att differentiera de åtgärder som får vidtas inom ramen för ingripanden enligt lagen. Mer ingripande åtgärder kräver som nämnts en mer kvalificerad beslutsfattare. Det bör därför inte göras någon skillnad i det avseendet beroende på om det är tekniskt och praktiskt möjligt att göra en kopia eller inte. Att låta frågan om vem som bör fatta beslut vara beroende av tekniska och praktiska förutsättningar är inte acceptabelt. Det skulle göra tillämpningen av lagen alltför slumpartad. Utredningen anser därför att beslutsfattandet inte bör delas upp på det angivna sättet.

Vilka åklagare bör besluta enligt lagen?

De uppgifter som ankommer på åklagare enligt den nya lagen skiljer sig från annan åklagarverksamhet. Det innebär att åklagaruppgiften sannolikt kommer att fullgöras av ett litet antal åklagare. Enligt utredningens mening finns det inte anledning att i författning styra vilka åklagare som bör ha den uppgiften. Riksåklagaren har möjlighet att närmare fördela åklagaruppgifterna och, om det behövs, utfärda föreskrifter eller allmänna råd avseende den nya arbetsuppgiften. Det får anses vara tillräckligt.

Polismyndigheten, Säkerhetspolisen respektive Tullverket bör initiera frågor om radering

Om åklagare ska besluta om radering behövs det bestämmelser om vilken myndighet som ska kunna initiera en sådan fråga. Eftersom beslut om andra ingripanden enligt den nya lagen än radering får fattas av befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket bör det föreskrivas att respektive myndighet ska

kunna initiera en fråga om radering. En ansökan om radering bör vara skriftlig och innehålla all den information som åklagaren behöver för att kunna ta ställning i frågan. Det innebär att det bör framgå av ansökan bl.a. vad syftet med raderingen är, vilka uppgifter som ska raderas och i vilket informationssystem (eller vilken del av systemet) som uppgifterna som ska raderas finns. Det bör även framgå hur raderingen ska genomföras, om beslut om radering fattas.

Det kan, som tidigare nämnts, förutses att frågan om ett ingripande i cybermiljö i form av radering kan komma att väckas t.ex. om det i en beslagtagen dator eller mobiltelefon finns material som bör raderas inte bara i den enheten utan även på en lagringstjänst, där det finns kopior av det. En enskild bör enligt utredningens mening inte kunna väcka en fråga om radering. Det ligger i linje med att enskilda normalt inte har någon initiativrätt när det gäller åtgärder inom brottsbekämpningen.

16.2.2 Intermistiska beslut om radering

Utredningens förslag

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för möjligheterna att förhindra förestående brott eller avbryta pågående brott i cybermiljö att inhämta åklagarens beslut, får särskilt utsedda befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket fatta interimistiskt beslut om radering och, i förekommande fall, även beslut om tillträde. Sådana beslut ska så snart som möjligt anmälas till åklagare.

Skälen för utredningens förslag

Interimistiska beslut om radering

Även om radering i många fall inte är lika brådskande som andra typer av ingripanden enligt den nya lagen, kan det finnas undantagsfall där raderingen behöver göras mer eller mindre omedelbart. Det behöver därför finnas möjlighet att mycket snabbt kunna besluta om radering. Genom systemet med jour och beredskap finns det, som tidigare nämnts, i princip åklagare som skulle kunna fatta beslut till-

gängliga dygnet runt. Även om en åklagare finns tillgänglig för beslut går det emellertid alltid åt viss tid för föredragningen. Det kan därför uppstå situationer där ingripandena är så brådskande att syftet med ingripandet riskerar att gå förlorat om det inte genomförs omedelbart. Det kan t.ex. röra sig om situationer där det finns en akut risk för att brott kan drabba människors liv eller hälsa eller brott som utgör ett akut hot mot rikets säkerhet. Terrorisminnehåll kan behöva raderas snabbt för att förhindra eller avbryta pågående terroristbrott och säkerhetskänslig information kan behöva raderas för att förhindra förestående brott eller avbryta grovt spionerі eller grov olovlig underrättelseverksamhet. Det kan vidare röra sig om en skadlig kod som behöver raderas för att förhindra eller avbryta pågående brott mot människors liv och hälsa eller egendom, där andra mindre ingripande åtgärder inte kan förväntas få avsedd effekt. Förutom att förhindra eller avbryta brott, kan en radering i ett enskilt fall ha akut skadebegränsande effekt, t.ex. genom att raderingen både förhindrar och minimerar risken för fortsatt spridning. Det kan i undantagsfall också röra sig om situationer där det av tekniska skäl endast under kort tid finns möjlighet att genomföra radering. För att tydliggöra att interimistiska beslut endast får fattas när det finns särskilda omständigheter bör krävas att det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för möjligheten att förhindra eller avbryta brott att avvakta åklagares beslut.

I de undantagsfall där radering måste utföras omedelbart bör därför särskilt utsedda befattningshavare hos Polismyndigheten, Säkerhetspolisen eller Tullverket kunna fatta interimistiska beslut om radering. Det bör, som tidigare nämnts, vara någon som dels har goda kunskaper om digitala informationssystem och informationssäkerhet, dels den särskilda kompetens, utbildning och erfarenhet som är nödvändig och även i övrigt är särskilt lämpad för att fatta beslut av komplicerad juridisk natur (se avsnitt 16.1).

Det bör ställas högre krav på risken för brott för att interimistiska beslut om radering ska få fattas. Det bör enligt utredningens mening antingen vara fråga om pågående brott som behöver avbrytas eller förestående brott som kan förhindras genom raderingen. På det sättet markeras att interimistiska beslut bör användas restriktivt.

I samband ett interimistiskt beslut om radering är det naturligt att särskilt utpekade befattningshavare vid Polismyndigheten, Säker-

hetspolisen och Tullverket, om det i ett enskilt fall behövs, även bör kunna fatta beslut om tillträde enligt den nya lagen.

Det bör ställas samma formella krav på ett interimistiskt beslut om radering och eventuellt beslut om tillträde som på beslut som fattas av åklagare. I avsnitt 17.1.2 anges vilket innehåll ett beslut om radering ska ha.

Underrättelse om interimistiska beslut till åklagare

Med hänsyn till att interimistiskt beslut om radering är ett undantag från huvudregeln att beslut om radering, och eventuellt beslut om tillträde som fattas i samband med det, ska fattas av åklagare, bör ett intermistiskt beslut så snart som möjligt skriftligen anmälas till åklagare för att han eller hon ska kunna pröva beslutet. Normalt krävs det inte att beslut som fattas i den brottsbekämpande verksamheten är motiverade, men ett sådant krav bör ställas i det här fallet.

16.2.3 Åklagare ska pröva interimistiska beslut

Utredningens förslag

Anmälan ska vara skriftlig och innehålla skälen för ingripandet. Om möjligt ska en kopia av de uppgifter som har raderats eller ska raderas fogas till anmälan.

Åklagaren ska så snart som möjligt pröva om det finns skäl för beslutet. Om åklagaren bedömer att sådana skäl saknas, ska han eller hon omedelbart upphäva beslutet.

Åklagaren ska säkerställa att kopior av raderade uppgifter förstörs senast sex månader efter prövningen.

Skälen för utredningens förslag

Åklagarens prövning av interimistiska beslut

När åklagaren underrättats om ett interimistiskt beslut om radering bör han eller hon så snart som möjligt pröva om det finns grund för beslutet. Enligt utredningens mening bör det inte krävas att en sådan

prövning görs under jourtid. Som tidigare nämnts kan det förutsättas att riksåklagaren utfärdar föreskrifter om vilka åklagare som ska pröva ingripanden enligt den nya lagen. Om det skulle röra sig om ett mindre antal åklagare är det inte givet att de alltid finns tillgängliga.

Åklagaren bör pröva beslutet på samma sätt som vid en ansökan om radering. Om åklagaren bedömer att det saknas grund för beslutet, bör han eller hon omedelbart upphäva det. Detsamma gäller ett eventuellt beslut om tillträde som har beslutats i samband med beslutet om radering.

Om uppgifterna i fråga redan har raderats när åklagaren ska pröva beslutet torde bli svårt för åklagaren att bedöma åtgärdens laglighet. En sådan prövning kan då bli illusorisk. För att kunna göra en rimlig prövning måste åklagaren därför ha någon form av underlag. Om de raderade uppgifterna inte finns tillgängliga för den ingripande myndigheten antingen i form av en kopia i något annat informationssystem än det som ingripandet har riktats mot eller i fysisk form bör det, om det är tekniskt möjligt, därför bevaras en kopia av de uppgifter som det intermistiska beslutet avser. För att åklagaren ska kunna bedöma om beslutet har varit lagligen grundat bör kopian fogas till anmälan. Om det inte är tekniskt möjligt att göra och bevara en sådan kopia, eller om en sådan åtgärd skulle riskera att avslöja arbetsmetoder som omfattas av sekretess, bör det på annat sätt dokumenteras vilka uppgifter som avses.

Utredningen återkommer i avsnitt 19.1.4 till frågan om underrättelse om interimistiska beslut om radering som redan har hunnit genomföras när åklagaren ska pröva det.

Bevarande och förstörande av kopior av raderade uppgifter

Vid kopiering kan de uppgifter som myndigheterna får tillgång till vara integritetskänsliga. Från den enskildes perspektiv kan en kopia som bevaras hos en brottsbekämpande myndighet därför, i likhet med ett beslag, innebära en inskränkning av hans eller hennes rätt till respekt för sitt privatliv enligt artikel 8.1 i Europakonventionen och 2 kap. 6 § RF (jfr Modernare regler för användningen av tvångsmedel, prop. 2021/22:119, s. 109). För att uppgifter inte ska bevaras i större omfattning än nödvändigt bör åklagaren därför säkerställa att

sådana kopior som har fogats till en anmälan förstörs. För att underlätta tillsyn bör kopior av raderade uppgifter bevaras viss tid (se avsnitt 19.3 om tillsyn). En rimlig lösning är att kopior av det slaget alltid ska förstöras efter sex månader. Det finns enligt utredningens mening inte något enskilt eller allmänt intresse som kräver att sådana kopior bevaras längre tid än så. Att sådana kopior förstörs har inte någon betydelse för t.ex. den enskildes rätt till en rättvis rättegång, eftersom ingripande i cybermiljö inte syftar till att utreda brott (jfr prop. 2021/22:119 s. 125 f. och prop. 2023/24:117 s. 138 f.). Utredningen återkommer i avsnitt 20.1 till hur ingripanden enligt den nya lagen förhåller sig till andra brottsbekämpande åtgärder.

16.2.4 Bör beslut om radering kunna överklagas?

Utredningens bedömning

Åklagares beslut om radering bör inte kunna överklagas eller på annat sätt prövas av någon fristående myndighet.

Skälen för utredningens bedömning

Bakgrund

En särskild fråga som väcks när det gäller beslut om radering enligt den nya lagen är vilka rättssäkerhetsgarantier som bör omgärda den nya regleringen. Till dem hör frågan om beslut om radering, som är den enda oåterkalleliga åtgärd som föreslås, bör få överklagas eller kunna prövas på annat sätt.

Få åklagarbeslut får överklagas

Allmänt sett kan konstateras att det är mycket få åklagarbeslut som får överklagas, trots att åklagare har omfattande beslutsbefogenheter. De åklagarbeslut som genom uttrycklig reglering får överklagas är sådana beslut som är överklagbara oavsett vilken myndighet som har fattat dem (t.ex. beslut i sekretessärenden). Däremot finns det

regler som i vissa fall ger möjlighet att, på annat sätt än genom överklagande, få till stånd rättens prövning av ett åklagarbeslut.

När det gäller straffprocessuella tvångsmedel finns det bestämmelser som gör det möjligt för den som har drabbats av vissa tvångsmedel, bl.a. reseförbud (25 kap. 5 § RB) och beslag (27 kap. 6 § RB) att begära rättens prövning av åtgärden. Den prövning som rätten då gör är att avgöra om tvångsmedlet ska bestå. Vidare kan rätten på en misstänkts begäran pröva om en förundersökning ska kompletteras (23 kap. 19 § RB) och om den brottsmisstänkte ska ges ökad insyn i förundersökningsmaterialet (23 kap. 21 d § RB). Det gäller inga särskilda tidsfrister för att begära rättens prövning av nu aktuellt slag.

Däremot gäller enligt 23 kap. 6 b § RB en tidsfrist på tre veckor för den som vill begära rättens prövning av ett av åklagare utdömt vite för att en person inte har inställt sig till förhör.

Det finns även andra åklagarbeslut som på begäran av den som är berörd ska prövas av domstol. Det rör sig om beslut där förvaltningslagen eller ärendelagen delvis ska tillämpas. Det gäller bl.a. beslut om kontaktförbud (14 § lagen [1988:688] om kontaktförbud) och beslut om vissa tillträdesförbud (13 § lagen [2005:321] om tillträdesförbud vid idrottsarrangemang och 13 § lagen [2021:34] om tillträdesförbud till butiker, badanläggningar och bibliotek). Inte heller i de fallen gäller någon särskild tidsfrist för att begära rättens prövning.

När det gäller förverkande finns det ett särskilt förfarande. Den som har fått ett förverkandebeslut som har meddelats av antingen en åklagare eller en polisman eller annan anställd vid vissa brottsbekämpande myndigheter får enligt 3 kap. 5 § lagen (2024:782) om förfarandet vid förverkande av egendom och åläggande av företagsbot anmäla missnöje hos den myndighet som har meddelat beslutet inom tre veckor. Om missnöje anmäls, upphör beslutet om förverkande att gälla. Åklagare kan senast inom en månad från missnöjesanmälan väcka talan om förverkande. Om talan inte väcks, är frågan om förverkande slutligt avgjord.

Överprövningsförfarandet

Inom åklagarväsendet finns sedan länge ett särskilt förfarande för omprövning av åklagarbeslut, nämligen det som brukar kallas överprövningsförfarandet. Det bygger på att åklagarväsendet är hierarkiskt uppbyggt och att vissa överordnade åklagare (överåklagare och riksåklagaren) enligt 7 kap. 5 § RB får överta en underordnad åklagares uppgifter. Överprövningsförfarandet är inte författningsreglerat, men det finns vissa av riksdagen fastlagda riktlinjer för prövningen. De innebär bl.a. att beslut som inte längre gäller inte överprövas. En begäran om överprövning av ett raderingsbeslut skulle därmed sannolikt inte överprövas.

Bör ett särskilt förfarande för prövning av åklagarbeslut införas?

Det som är gemensamt för de, ganska få, situationer där någon i dag kan begära rättens prövning av ett åklagarbeslut är dels att det är fråga om beslut som har betydande verkan för den enskilde, dels att det är en pågående åtgärd eller inskränkning av den enskildes fri- och rättigheter. Så är emellertid inte fallet vid radering. Det är ett beslut som i stället närmast kan liknas vid förverkande, som är ett förfarande där den som utsätts för åtgärden, slutligt går miste om något.

En första fråga är därför om regleringen avseende förverkandebeslut kan tjäna som förebild. Enligt utredningens mening är det inte någon rimlig lösning, eftersom den regleringen bygger på att beslut om förverkande normalt meddelas av domstol på talan av åklagare. I de fall där beslut om förverkande meddelas på lägre nivå och ett sådant beslut bestrids av den som beslutet har riktats mot förutsätts åklagaren väcka talan vid domstol om förverkande. Regleringen bygger alltså på ett helt annan typ av förfarande och kan därför inte överföras till den nya lagen.

Nästa fråga är om det finns något annat lämpligt sätt att bringa åklagarbeslut om radering under domstolsprövning. När ett ingripande i cybermiljö görs kommer det sannolikt endast i undantagsfall att finnas någon koppling till en pågående förundersökning. Även om vissa av ingripandena så småningom kan leda till att en förundersökning inleds, kan frågan om radering vara något som ändå inte kommer att hanteras i förundersökningen. Med domstolsprövning kommer frågan om radering att hållas öppen länge. Oavsett vilken

typ av uppgifter som ska raderas kan en sådan fördröjning inte antas vara till fördel vare sig för brottsbekämpningen eller för de enskilda vilkas uppgifter kan förekomma i materialet. Typiskt sett kan radering avse personuppgifter som har kommit i kriminellas händer och som kan komma att missbrukas av dem, övergreppsmaterial som av hänsyn till berörda bör raderas så snart som möjligt, skadlig kod som kan komma att användas vid brott eller säkerhetskänsligt material som bör raderas för att inte komma i främmande makts händer. Mot den bakgrunden anser utredningen att det inte bör införas någon särskild möjlighet att föra talan i domstol angående beslut om radering.

Det finns inte heller skäl att införa ett förfarande där någon annan fristående myndighet än domstol ges i uppgift att överpröva åklagares beslut om radering enligt den nya lagen.

17 Besluten

17.1 Formella krav på beslut

17.1.1 Muntliga eller skriftliga beslut?

Utredningens förslag

Ett beslut om ingripande enligt den nya lagen ska vara skriftligt. Om det skulle medföra en fördröjning av väsentlig betydelse för syftet med ingripandet får beslutet meddelas muntligen. Det ska då dokumenteras så snart som möjligt och ska ha samma innehåll som ett skriftligt beslut.

Skälen för utredningens förslag

Det finns inget allmänt krav på att beslut som fattas av en brottsbekämpande myndighet ska vara skriftliga. Förvaltningslagens (2017:900) regler om handläggning är nämligen inte tillämpliga på brottsbekämpande verksamhet (3 § förvaltningslagen). Vid vissa åtgärder ställs det emellertid krav på dokumentation enligt bl.a. RB och polislagen. Det gäller framför allt åtgärder som innebär inskränkningar i grundläggande fri- och rättigheter. I motsats till det som gäller för bl.a. domstolar ställs det inte heller något generellt krav på att beslut alltid ska motiveras.

Av integritets- och rättssäkerhetsskäl är det viktigt att beslut om ingripanden i cybermiljö är skriftliga. Det lämnar inte någon osäkerhet om vad ingripandet omfattar och underlättar för dem som ska genomföra det. Det finns emellertid situationer som kräver att beslut enligt lagen meddelas mycket snabbt, eftersom syftet med ingripandet annars kan förlora sin betydelse. I sådana fall bör beslutet kunna fattas muntligen, men därefter dokumenteras så snart som

möjligt och ha samma innehåll som ett skriftligt beslut. Det ligger väl i linje med de dokumentationskrav som gäller enligt RB.

17.1.2 Innehållet i beslut

Utredningens förslag

I beslut om ingripande ska följande anges:

1. ändamålet med ingripandet,
2. vilket brott eller vilken brottslig verksamhet som ingripandet avser,
3. vilket informationssystem och, om möjligt, vilken avgränsad del av informationssystemet som ingripandet avser,
4. vilken åtgärd som ingripandet omfattar,
5. när ingripandet senast ska genomföras,
6. de villkor som gäller för ingripandet, och
7. om ett beslut om tillträde enligt lagen har fattats och vilken plats det i sådana fall omfattar.

Tiden enligt punkten 5 får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet.

Skälen för utredningens förslag

Vilka uppgifter som bör anges i besluten

Utgångspunkten är att endast de uppgifter som behövs för att genomföra ett ingripande bör anges i ett beslut om ingripande enligt den nya lagen. Ett grundläggande krav på ett sådant beslut bör vara att det anger vilket informationssystem som ingripandet avser. Om det är möjligt bör det framgå vilken avgränsad del av systemet som avses. Det kan t.ex. vara fråga om ett visst användarkonto, ett visst program, en viss hemsida eller någon annan närmare specificerad del av informationssystemet. Det är likaså viktigt att det i beslutet anges vad som är ändamålet med ingripandet och vilka åtgärder som får

vidtas. Genom det sätts ramarna för vad ingripandet kan avse. Vidare bör det framgå vilket brott eller vilken brottslig verksamhet som ingripandet avser. Andra frågor som har betydelse för att genomföra ett ingripande, bl.a. vilka andra förutsättningar och villkor som gäller, bör också anges i beslutet.

Eftersom de omständigheter som är avgörande för frågan om den nya lagen är tillämplig saknar betydelse för möjligheterna att genomföra ett ingripande, finns det enligt utredningens mening inte något behov av att de anges i beslutet. Däremot kan särskilda omständigheter som har påverkat frågan om lagen är tillämplig behöva dokumenteras på annat sätt, se avsnitt 19.2.

Av beslutet om ingripande bör det alltid framgå om beslut om tillträde har fattats och vilken plats det i så fall avser.

Bör det anges en tidsram för hur länge försök till ingripande får göras?

Ett ingripande i cybermiljö är i många fall komplext och kan därför ta tid att faktiskt genomföra. Det kan kräva förberedelsetid, där de tekniska förutsättningarna för ingripandet undersöks, för att aktsamhetskrav (se avsnitt 18.3) och eventuella villkor (se avsnitt 17.2) ska kunna uppfyllas. Det kan även finnas begränsat tidsutrymme att för att genomföra ingripandet, beroende på om säkerhetsskydd behöver brytas. En särskild fråga är därför om det i ett beslut om ingripande bör anges under vilken tid som ingripandet får genomföras. Det kan synas motsägelsefullt, eftersom ingripanden enligt den nya lagen förutsätts vara kortvariga och beslutsfattaren och den som ska genomföra ingripandet normalt finns i samma myndighet, men det har sin grund i de praktiska problem som är förknippade med genomförandet.

I beslut om hemliga tvångsmedel ska det alltid anges vilken tid tillståndet att använda tvångsmedlet avser. Tiden får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet (se bl.a. 27 kap. 21 § andra stycket RB). När det gäller hemlig dataavläsning har en annan lösning valts, nämligen att det i beslut om tvångsmedlet ska anges under vilken tid som tvångsmedlet får verkställas (18 § första stycket 1 lagen om hemlig dataavläsning). Det beror på att det

tvångsmedlet, på ett helt annat sätt än andra tvångsmedel, är beroende av de tekniska möjligheterna att verkställa det.

Även om det inte genomgående är rimligt att jämföra ingripanden enligt den nya lagen med det som gäller för hemliga tvångsmedel, där besluten normalt fattas av en myndighet och verkställs av en annan, finns det vissa problem som är gemensamma. Dit hör frågan om det bör sättas gränser för hur länge försök att genomföra ingripandet får pågå. Av rättssäkerhetsskäl bör det enligt utredningens mening anges i beslut om ingripanden i cybermiljö vilken tidsram som gäller för att försöka genomföra ingripandet. Annars finns det risk för att ett ingripande inte avslutas tillräckligt snabbt eller att det förlorar i aktualitet på ett sätt som inte har varit avsett. Det bör därför i ett beslut enligt den nya lagen anges när ingripandet senast ska genomföras. Tiden för genomförande bör inte vara längre än nödvändigt och inte vara längre än en månad från dagen för beslutet.

17.2 Villkor

Utredningens förslag

I ett beslut om ingripande ska det, när det finns skäl till det, anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

Skälen för utredningens förslag

Villkor fyller en viktig funktion

Att ett ingripande ska riktas mot ett visst informationssystem, eller en viss närmare avgränsad del av det, innebär i sig att risken för onödiga integritetsintrång minskar, eftersom åtgärden är begränsad till de uppgifter som finns där. Även med den begränsningen kan emellertid målet för ett ingripande innehålla stora mängder information. Det är inte säkert att all information i ett informationssystem behöver gås igenom för att uppnå syftet med ingripandet, men det kan samtidigt vara svårt att avgränsa beslutet på ett adekvat sätt. Då kan villkor för hur ingripandet får genomföras bidra till att begränsa integritetsintrånget.

Bör det vara obligatoriskt med villkor?

En första fråga är om det bör vara obligatoriskt med villkor vid ingripanden i cybermiljö. För- och nackdelarna med obligatoriska villkor diskuterades ingående när regleringen om hemlig dataavläsning permanentades (se prop. 2024/25:51 s. 54 f.). Det kan nämligen i vissa fall kan vara svårt, och ibland omöjligt, att vid beslutstillfället formulera adekvata villkor. Om det ställs krav på att villkor ska vara obligatoriska kan det i sin tur leda till att respekten för regleringen urholkas, eller att de villkor som anges saknar faktiskt innehåll. Mot den bakgrunden anser utredningen att det bör ställas krav på att beslutsfattaren alltid överväger om villkor bör ställas, men att villkor inte bör vara ett absolut krav för beslut om ingripande enligt lagen.

Villkor bör alltid övervägas

I fall där det kan antas att ett informationssystem innehåller en mängd integritetskänsliga uppgifter bör det enligt utredningens mening krävas att beslutsfattaren alltid överväger om det i beslutet om ingripande bör anges särskilda villkor för att säkerställa att enskildas personliga integritet inte kränks i onödan. Förutom att villkor minskar risken för onödiga integritetsintrång kan villkor även ha betydelse för bedömningen om ett ingripande är proportionerligt. Det är dock viktigt att villkoren i beslut utformas med tillräcklig precision och tydlighet, så att de får ett faktiskt innehåll men samtidigt inte hindrar att ingripandet kan genomföras (jfr Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott, prop. 2022/23:126, s. 154 och prop. 2024/25:51 s. 54 f.).

Villkor kan ta sikte på i stort sett vilka omständigheter som helst som kan gagna skyddet för den personliga integriteten. Det gäller särskilt om åtgärderna riktar sig mot ett informationssystem som används av en större krets av personer, exempelvis en webbplats, eller ett informationssystem som kan antas innehålla särskilt känslig information om enskilda personer. Det är emellertid tänkbart att den ingripande myndigheten inte på förhand har en tillräckligt god bild av informationssystemet med hänsyn till det tidiga skede i vilket ingripanden görs. Det kan göra det svårt att formulera adekvata villkor. Utgångspunkten bör dock vara att beslutsfattaren ska försöka begränsa ingripandet genom villkor när det är möjligt.

När det gäller beslut om radering kan det förefalla som om villkor skulle vara överflödiga. I det fallet kan emellertid villkor användas för att avgränsa t.ex. vilka specifika uppgifter som ska raderas.

Situationen kan dock vara den att villkor anses vara obehövliga i fall där myndigheterna har vederhäftig information om att informationssystemet endast används i brottsligt syfte. Det kan vara fallet om åtgärden riktas mot vissa informationssystem, t.ex. webbplatser på Darknet som förmedlar kriminella tjänster eller chattkonton som enbart används för kommunikation mellan kriminella.

Vid utformningen av villkoren bör det beaktas att begränsande villkor kan försvåra verkställigheten. En bedömning måste alltid göras i det enskilda fallet. Med hänsyn till det som nyss sagts bör villkor endast anges när det är aktuellt.

17.3 Beslut om tillträde

17.3.1 Beslut om tillträde till vissa platser

Utredningens förslag

Om det är nödvändigt för att genomföra ett ingripande enligt den nya lagen får den ingripande myndigheten, efter särskilt beslut om tillträde, i hemlighet bereda sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång.

Beslut om tillträde får endast avse en plats där det finns särskild anledning att anta att informationssystemet finns tillgängligt. Om platsen är någons stadigvarande bostad, får beslut fattas endast om det finns synnerlig anledning att anta att informationssystemet finns tillgängligt där.

Skälen för utredningens förslag

Beslut om tillträde kan behövas

Ingripanden i cybermiljö kan göras på olika sätt. Ibland kan det krävas att den ingripande myndigheten bereder sig tillgång till en plats där det informationssystem eller den tekniska utrustning finns som ingripandet riktar sig mot. I andra fall kan myndigheten ha behov av

att få tillgång till en plats för att där installera viss utrustning, som är nödvändig för att kunna verkställa ingripandet.

Ett motsvarande behov finns när det gäller användning av vissa hemliga tvångsmedel. Enligt 12 § lagen om hemlig dataavläsning får den verkställande myndigheten vid hemlig dataavläsning, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Liknande bestämmelser om tillträdestillstånd för verkställighet av hemlig kameraövervakning eller hemlig rumsavlyssning finns i 27 kap. 25 a § första stycket RB.

Tillträde till platser som allmänheten inte har tillgång till

För att ett ingripande i cybermiljö ska få avsedd effekt behöver det enligt utredningens mening i vissa fall kunna kombineras med ett beslut om rätt att bereda sig tillträde till annars skyddade utrymmen (jfr prop. 2019/20:64 s. 143 f.). Vid verkställighet av tillstånd enligt den nya lagen kan den ingripande myndigheten ha behov av att komma nära informationssystemet eller att tillfälligt ha det i fysisk besittning, t.ex. om hårdvara ska användas vid ingripandet eller när det inte är möjligt att på distans installera programvara. Ett sätt att möjliggöra ingripandet i sådana situationer är att tillåta den brottsbekämpande myndigheten att bereda sig tillträde till utrymmen som annars är skyddade mot intrång enligt bl.a. reglerna i 4 kap. brottsbalken. Som konstaterats i tidigare lagstiftningsärenden utgör beslut om tillträde ingen utvidgning av möjligheterna att ingripa och ökar därmed inte i sig risken för integritetsintrång. Frågan om tillträde ska alltid bedömas fristående, med utgångspunkt i omständigheterna i det enskilda fallet.

Regleringen om beslut om tillträde bör enligt utredningens mening utformas med regleringen om hemlig dataavläsning som förebild. Det innebär att det bör krävas att det finns särskild anledning att anta att informationssystemet, som ingripandet ska riktas mot, finns på den plats som beslutet avser. Det ska därmed finnas någon faktisk omständighet som med viss styrka talar för att informationssystemet kommer att finnas tillgängligt där, i vart fall någon gång

under den tid som ingripandet får genomföras (jfr prop. 2019/20:64 s. 144).

Ett beslut om tillträde till en viss plats kan vara mindre integritetskränkande än tillträde till en annan plats. Det följer då av proportionalitetsprincipen att den minst integritetskänsliga platsen ska väljas i första hand.

Till skillnad från verkställighet enligt lagen om hemlig dataavläsning, där tvångsmedlet alltid verkställs utan den misstänktes vetskap och det därför finns en bestämmelse om tillträde i hemlighet, torde det bara i vissa fall vara nödvändigt att fatta beslut om tillträde vid ingripanden i cybermiljö. Det aktualiseras bara om den ingripande myndigheten fysiskt behöver installera tekniska hjälpmedel. Om ingripandet kan genomföras digitalt behövs det inget sådant beslut. Något beslut om tillträde behövs inte heller om installationen av hjälpmedlet kan göras med samtycke av den som förfogar över lokalen. På samma sätt som ett beslut om ingripande i fysisk miljö behövs det alltså inget beslut om tillträde om den som förfogar över den lokal där hjälpmedlet ska installeras förväntas samarbeta med den ingripande myndigheten. Om däremot samtycke inte kan förväntas, eller det kan antas motverka syftet med ingripandet att inhämta samtycke, behövs det möjlighet att besluta om tillträde. För att göra det tydligt att myndigheten, i de undantagsfall där det behövs, får bereda sig tillträde i hemlighet bör det framgå av lagtexten. En bedömning får ske i varje enskilt fall om ett beslut om tillträde behövs.

Beslut om tillträde till någons stadigvarande bostad

Det finns enligt utredningens mening skäl att göra skillnad på tillträde till platser som utgör någons stadigvarande bostad och andra platser, eftersom intrång i sådana bostäder utgör ett större ingrepp i den personliga integriteten. Även här kan en jämförelse göras med det som gäller för hemlig dataavläsning. Ett beslut om tillträde till en bostad för att verkställa hemlig dataavläsning får, enligt 12 § lagen om hemlig dataavläsning, endast beviljas om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller, i underrättelseverksamhet, den person som tvångsmedlet riktas mot. En förutsättning är vidare att det finns synnerlig anledning att anta att informationssystemet finns tillgängligt där. I förarbetena utta-

lade regeringen att det bör ställas ytterst höga krav för sådant tillträdestillstånd (prop. 2019/20:64 s. 145). För hemlig dataavläsning i inhämtningslagsfallen ansågs det dock inte lämpligt med en reglering som gör skillnad på i vems bostad informationssystemet finns, eftersom inhämtningen inte har någon koppling till en viss person och det därför var svårt att se hur beviströsklarna skulle kunna differentieras i olika personers bostäder.

Samma höga krav bör ställas vid ett beslut om tillträde vid ingripanden i cybermiljö som vid verkställighet av hemlig dataavläsning. Det bör alltså finnas synnerlig anledning att anta att informationssystemet som ingripandet riktas mot finns i bostaden för att beslut om tillträde till någons stadigvarande bostad ska få fattas. Synnerlig anledning är ett högt beviskrav och förutsätter att det ska vara så gott som säkert att informationssystemet finns tillgängligt i bostaden i fråga.

17.3.2 Förbud mot tillträde till vissa platser

Utredningens förslag

Beslut om tillträde får inte avse en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet

1. där tystnadsplikt gäller enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL,
2. som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2025:400) eller av rättegångsombud, deras biträden och försvarare som inte är advokater, eller
3. som bedrivs av präster inom trossamfund, eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Skälen för utredningens förslag

I avsnitt 15.2 har utredningen föreslagit att ingripanden inte får avse informationssystem som stadigvarande används eller är särskilt avsedda att användas i verksamheter som omfattas av regleringen i 36 kap. 5 § femte och sjätte styckena RB. Det ligger i sakens natur att beslut om tillträde inte heller bör få avse platser där sådana verksamheter bedrivs. Av tydlighetsskäl bör det framgå av den nya lagen att ett beslut om tillträde inte får avse platser som stadigvarande används eller är särskilt avsedda att användas för de verksamheter som omfattas av regleringen i 36 kap. 5 § femte och sjätte styckena RB.

Utredningen har inte föreslagit något generellt förbud mot ingripanden mot informationssystem som används eller är avsedda att användas i de verksamheter som omfattas av regleringen i 36 kap. 5 § andra och tredje styckena RB (se avsnitt 15.2). Det väcker frågan hur långt förbudet mot tillträde till vissa platser bör sträcka sig. Även om förbudet mot ingripanden är snävare formulerat och proportionalitetsprincipen i de flesta fall torde hindra att beslut om tillträde ges till platser där sådana verksamheter som anges i 36 kap. 5 § andra och tredje styckena RB bedrivs, finns det enligt utredningens mening skäl att uttryckligen föreskriva att beslut om tillträde inte får ges till sådana platser. På en plats där det stadigvarande bedrivs sådan verksamhet kan det nämligen förutsättas att det finns betydande mängder särskilt integritetskänslig information.

18 Verkställighet

18.1 När ingripanden får genomföras

Utredningens förslag

Beslut om ingripanden enligt den nya lagen får verkställas omedelbart, om inte annat anges.

Skälen för utredningens förslag

Ingripanden med stöd av den nya lagen måste i många fall göras snabbt och behöver därmed kunna genomföras omedelbart. I de fall där det anses vara viktigt att avvakta med att genomföra ett ingripande bör det dock finnas möjlighet till det. Ett exempel kan vara att ingripandet behöver samordnas med någon annan brottsbekämpande åtgärd, att det är fråga om ett ingripande där flera länders brottsbekämpande insatser samordnas eller att det av något annat skäl finns anledning att välja en framtida tidpunkt för ingripandet.

Ett beslut om ingripande bör enligt utredningens mening inte kunna användas för att vid upprepade tillfällen vidta åtgärder i det system som den brottsbekämpande myndigheten har berett sig tillgång till. På samma sätt som beslut vid ingripanden i den fysiska miljön bara gäller där och då, eftersom förutsättningarna för ingripandet snabbt kan förändras, bör ett ingripande i cybermiljön bara omfatta den eller de åtgärder som vidtas vid själva ingripandet. Avsikten med regleringen är alltså inte att ett beslut om ingripande ska kunna utnyttjas vid flera tillfällen. I stället får ett nytt beslut fattas om det visar sig att åtgärder, som inte kunde förutses vid det ursprungliga beslutet, behövs.

En helt annan sak är att det kan krävas tid och planering innan ett ingripande genomförs. Det beror på att den ingripande myndigheten kan behöva utnyttja sårbarheter i det informationssystem som ingripandet riktas mot eller avvakta med att ingripa tills ett inaktivt informationssystem är i drift eller av annat skäl invänta det mest lämpliga tillfället att ingripa.

18.2 Metoder för genomförande

Utredningens förslag

När ingripanden genomförs får de tekniska hjälpmedel som behövs användas. Systemskydd får brytas eller kringgås och tekniska sårbarheter får utnyttjas.

Om ett tekniskt hjälpmedel har installerats, ska hjälpmedlet tas bort eller göras obrukbart så snart som möjligt efter det att ingripandet har genomförts eller beslutet om ingripande har upphört att gälla.

Skälen för utredningens förslag

Användning av tekniska hjälpmedel

Den nya regleringen är, som påpekats i avsnitt 14.2, teknikneutral. Utredningen anser därför att det inte behövs några bestämmelser om tekniska aspekter på hur ingripandet får genomföras, utöver att det bör föreskrivas att de tekniska hjälpmedel som behövs för genomförandet får användas. Det innebär att den ingripande myndigheten får bereda sig tillgång till informationssystem och uppgifter i sådana system genom olika tekniska eller administrativa lösningar.

Som framgått av avsnitt 14.2 ger den nya lagen den ingripande myndigheten rätt att bereda sig tillgång till uppgifter i ett informationssystem utan att göra sig skyldiga till dataintrång. Begreppet bereda sig tillgång till innebär i detta sammanhang att myndigheten – oftast utan att den som äger eller använder det informationssystem som ingripandet riktas mot vet om det – genom en teknisk åtgärd eller på något annat sätt skaffar sig tillgång till hela eller delar av syste-

met. På så sätt blir det möjligt för myndigheten att vidta ytterligare åtgärder i informationssystemet.

Det bör av tydlighetsskäl framgå av den nya lagen att den ingripande myndigheten har rätt att kringgå eller bryta systemskydd. Vilka tekniska eller andra metoder som myndigheten får använda bör, som nyss nämnts, inte regleras närmare. Att kringgå eller bryta systemskydd innebär att myndigheten genom avancerade tekniska åtgärder får bereda sig tillgång till informationssystemet, t.ex. genom att installera ett särskilt program och på så sätt t.ex. ta sig förbi en multifaktorautentisering.

Det bör vidare framgå att myndigheten har rätt att utnyttja sårbarheter i informationssystem, alltså omständigheter som gör systemen känsliga för angrepp. Det kan röra sig om både tekniska brister, bl.a. bristfälliga och osäkra system, och mänskliga svagheter, som slarv och tanklöshet (jfr prop. 2019/20:64 s. 57, 160 och 235).

Det är viktigt att framhålla att den ingripande myndigheten även får bereda sig tillgång till uppgifter i ett informationssystem utan tekniskt avancerade åtgärder på samma sätt som en vanlig användare. Det kan göras genom att logga in med användarnamn och lösenord, klicka på en applikation eller på liknande sätt öppna den fil, det program eller den applikation som ingripandet avser. Som tidigare nämnts kan myndigheten även använda funktionen för att byta lösenord för att bereda sig tillgång till ett informationssystem eller för att tillfälligt blockera användarens tillgång till systemet.

Åtgärder när ingripandet har avslutats

Vid bl.a. hemlig dataavläsning, som också riktar sig mot informationssystem, ställs det krav på att ett tekniskt hjälpmedel som har använts för verkställigheten ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter det att tiden för tillståndet har gått ut eller tillståndet har upphävts (25 § tredje stycket lagen om hemlig dataavläsning). Eftersom det vid verkställighet av hemlig dataavläsning kan komma i fråga att använda programvara som har installerats utan fysisk tillgång till det informationssystem som avses, ansågs det vara tillräckligt med avinstallation av programvaran.

Utredningen anser att det finns samma behov av reglering av hur de brottsbekämpande myndigheterna ska förfara med sådana tekni-

ska hjälpmedel som myndigheterna har installerat när ett ingripande i cybermiljö har avslutats. Det bör därför föreskrivas att om ett tekniskt hjälpmedel har installerats, ska hjälpmedlet tas bort eller göras obrukbart så snart som möjligt efter det att ingripandet har genomförts eller beslutet om ingripande har upphört att gälla. Det innebär t.ex. att myndigheten ska ta bort kryptering som den har lagt till och återställa systemet till tidigare krav på autentisering.

18.3 Aktsamhetskrav

Utredningens förslag

När ett ingripande enligt lagen genomförs får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Ingripandet ska genomföras på sådant sätt att påverkan på annan som använder samma del av informationssystemet blir så begränsad som möjligt.

Skälen för utredningens förslag

Möjligheten för en ingripande myndighet att bereda sig tillgång till informationssystem bör kombineras med aktsamhetskrav som begränsar hur verkställigheten närmare får utformas. Det ligger nämligen i sakens natur att en myndighet, som bereder sig tillgång till ett informationssystem för att vidta åtgärder i systemet, kan orsaka skada eller olägenhet för den som äger eller använder informationssystemet. Det kan till och med vara det direkta syftet med en åtgärd, t.ex. vid blockering eller radering av uppgifter i informationssystemet. Proportionalitetsprincipen innebär att det minst ingripande sättet att genomföra ingripandet ska väljas. Enligt utredningens mening finns det behov av att, på samma sätt som gäller vid verkställighet av bl.a. hemliga tvångsmedel, ställa vissa krav på hur ett ingripande får genomföras (jfr bl.a. 27 kap. 25 a § femte stycket RB och 25 § lagen om hemlig dataavläsning). Det bör krävas att ingripanden i cybermiljö genomförs på ett sådant sätt att olägenhet eller skada inte orsakas utöver vad som är absolut nödvändigt. Som påpekats har syftet med åtgärden stor betydelse för bedömningen av

om skadan eller olägenheten går utöver vad som är absolut nödvändigt.

Utredningen har övervägt om de aktsamhetskrav som anges i 25 § andra stycket lagen om hemlig dataavläsning även bör gälla enligt den nya lagen. Enligt den bestämmelsen ska den verkställande myndigheten, när verkställigheten avslutas, vidta de åtgärder som behövs för att informationssäkerheten i det informationssystem som har avlästs ska hålla minst samma nivå som vid verkställighetens början. Det kravet bör ses mot bakgrund av att hemlig dataavläsning kan vara en betydligt mer ingripande åtgärd med en verkställighet som pågår under en längre tid och att tvångsmedlet kan verkställas vid upprepade tillfällen under den tiden. Ingripanden i cybermiljö har en annan karaktär. Det ligger för det första i sakens natur att uppgifter som har raderats inte bör återställas. Det skulle direkt motverka syftet med ingripandet. För det andra avser begreppet informationssäkerhet inte bara konfidentialitet utan även tillgänglighet och riktighet. Eftersom ingripanden enligt den nya lagen, förutom radering, kan avse ändring eller blockering är det uppenbart att informationssäkerheten, såvitt avser tillgänglighet och riktighet, inte kan återställas. Kravet i lagen om hemlig dataavläsning har också enligt uppgift visat sig vara problematiskt i praktiken. Utredningen anser därför att ett sådant krav inte bör ställas på de kortvariga ingripanden som nu är aktuella.

Ett ingripande kan rikta sig mot ett informationssystem som är tillgängligt för flera personer. Ingripandet kan också rikta sig mot en begränsad del av ett större informationssystem, exempelvis ett användarkonto till en kommunikationstjänst, lagringstjänst eller internetbaserade tjänster som används för kommunikation eller lagring. Det kan uppstå situationer där inte samtliga användare av kontot kan knytas till det brott eller den brottsliga verksamhet som ingripandet avser. I sådana fall är det enligt utredningens mening särskilt viktigt att den ingripande myndigheten i möjligaste mån begränsar den påverkan på andra personers användning av informationssystemet som ett ingripande kan få. Det bör därför föreskrivas att åtgärderna ska verkställas på sådant sätt att påverkan på annan som använder samma del av informationssystemet blir så begränsad som möjligt. Det bör emellertid påpekas att vissa ingripanden kan vara avsedda att direkt påverka andras användning av ett informationssystem. Det kan t.ex. vara syftet med att blockera tillgången till en marknadsplats, för att

förhindra försäljning av illegala varor, eller att blockera tillgången till terrorisminnehåll, för att förhindra bombtillverkning. Den nu aktuella begränsningen är givetvis inte avsedd att träffa ingripanden som görs i sådana syften.

18.4 Skyldighet att medverka

Utredningens förslag

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § LEK ska på begäran av den ingripande myndigheten vara skyldig att medverka när ingripanden enligt den nya lagen aktualiseras.

Den som medverkar ska ha rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den ingripande myndigheten.

Skälen för utredningens förslag

Operatörer bör vara skyldiga att medverka

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § LEK är på begäran av en verkställande myndighet skyldig att medverka i samband med verkställighet av hemlig avlyssning och hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning. Den som medverkar har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten.

I förarbetena till 24 § lagen om hemlig dataavläsning konstaterades att brottsbekämpande myndigheter behöver operatörens medverkan för att kunna installera de tekniska hjälpmedel som ska användas vid hemlig dataavläsning på ett så effektivt, snabbt och säkert sätt som möjligt. Om en operatör inte medverkar kommer verkställigheten av hemlig dataavläsning i vissa fall inte att kunna genomföras eller kräva tillstånd under betydligt längre tid. Det kan leda till att mer komplicerade metoder behöver användas, vilket kan innebära att de tekniska hjälpmedel som föranleder minst risker i verkställighetsfasen inte kan användas. Det kan i förlängningen ge upphov till

större risker för informationssäkerheten och den personliga integriteten än vad som annars hade uppstått (prop. 2019/20:64 s. 178).

Liknande behov av aktiv medverkan från operatörer finns enligt utredningens mening när det gäller Polismyndighetens, Säkerhetspolisens och Tullverkets förutsättningar att kunna genomföra ingripanden i cybermiljö. De kan t.ex. behöva få information som gör det möjligt att närmare identifiera det informationssystem som är målet för ingripandet eller att få annan nödvändig information för att kunna begränsa ingripandet. Det som har sagts om verkställighet av hemlig dataavläsning och valet av de tekniska hjälpmedel som innebär minst risk för onödigt integritetsintrång är lika relevant vid ingripanden enligt den nya lagen. Det kan dock antas att behovet av medverkan inte är lika omfattande vid tillämpning av den nya lagen som vid hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning av kommunikationsavlyssningsuppgifter och kommunikationsövervakningsuppgifter. Skyldigheten att medverka påverkar inte operatörernas skyldighet att lagra trafikuppgifter.

På samma sätt som vid verkställighet av hemliga tvångsmedel bör en bestämmelse om medverkan föreskriva en skyldighet för operatörerna att medverka. Den bestämmelsen bör placeras i 9 kap. LEK, där motsvarande medverkan beträffande hemliga tvångsmedel regleras. Medverkan av den enskilde operatören ska vara nödvändig och proportionerlig och endast de tekniska hjälpmedel som behövs för åtgärden får användas. När ett ingripande genomförs bör inte heller olägenhet eller skada få orsakas, utöver vad som är absolut nödvändigt. Det behövs även en följdändring i 9 kap. 21 § LEK.

Frågan om medverkan bör, på samma sätt som vid användning av hemliga tvångsmedel, väckas av den ingripande myndigheten när den konstaterat att operatörens medverkan i något avseende behövs för att kunna genomföra ingripandet. Den berörda operatören bör bistå enligt den ingripande myndighetens begäran när det gäller information som redan finns tillgänglig. Sådan medverkan kan t.ex. omfatta att operatören

- tillhandahåller tillgänglig teknisk information om det informationssystem som omfattas av beslutet om ingripande,

- tillhandahåller tillgängliga upplysningar om vilka förbindelser som används av det informationssystem som omfattas av beslutet om ingripande,
- använder tillgängliga tekniska metoder eller tillhandahåller möjlighet att använda sådana metoder, eller
- tillhandahåller andra liknande tillgängliga åtgärder som kan användas för att genomföra beslutet om ingripande.

Utredningen återkommer i avsnitt 20.4.2 till frågan om operatörernas tystnadsplikt.

Ersättning för medverkan

På samma sätt som vid verkställighet av vissa hemliga tvångsmedel, bör den ingripande myndigheten betala ersättning till operatören för sådana faktiska kostnader som uppstår vid medverkan (jfr prop. 2019/20:64 s. 180). Typiskt sett torde sådana kostnader avse att operatörens anställda tas i anspråk, men även andra faktiska kostnader som uppstår för operatören bör ersättas. Ersättningsfrågan bör normalt kunna lösas i samförstånd mellan myndigheten och den operatör som medverkar. På samma sätt som gäller för operatörernas medverkan vid verkställighet av hemliga tvångsmedel bör det finnas möjlighet för en myndighet att, efter bemyndigande, kunna utfärda närmare föreskrifter (jfr SOU 2017:89 s. 430). Den uppgiften bör ankomma på Post- och telestyrelsen, som har motsvarande uppgift när det gäller hemliga och preventiva tvångsmedel på teleområdet.

Det krävs ett bemyndigande

Enligt 8 kap. 7 § RF får regeringen meddela föreskrifter som inte enligt grundlag ska meddelas av riksdagen (den s.k. restkompetensen). Till restkompetensen hör sådana offentligrättsliga föreskrifter som inte rör förhållandet mellan enskilda och det allmänna utan avser de statliga myndigheternas organisation, arbetsuppgifter och inre verksamhetsformer. Till restkompetensen hör också sådana föreskrifter som visserligen rör förhållandet mellan enskilda och det allmänna men som ur den enskildes synpunkt inte är betungande, utan gyn-

nande eller neutrala. Med hänsyn till det nyss sagda bör det i den nya lagen införas ett bemyndigande för regeringen, eller den myndighet som regeringen bestämmer, att meddela närmare föreskrifter om operatörers medverkan. Det möjliggör att detaljerna för medverkan kan regleras i förordning (jfr 3 § förordningen [2020:172] om hemlig dataavläsning).

Bör andra än operatörer ha samma skyldighet?

Både Polismyndigheten och Säkerhetspolisen har särskilt lyft att skyldigheten att medverka vid ingripanden i cybermiljö inte bara bör omfatta de som enligt 2 kap. 1 § LEK tillhandahåller vissa kommunikationsnät eller tjänster som inte är nummeroberoende interpersonella kommunikationstjänster. Skyldigheten bör enligt myndigheternas uppfattning även omfatta de som inom svensk jurisdiktion lagrar data, s.k. värdtjänstbolag. De bör åläggas att lämna de upplysningar som behövs för att myndigheten ska kunna lokalisera och rikta ingripanden mot en server.

Ett värdtjänstbolag är ett bolag som t.ex. hyr ut serverutrymme, ibland kallat webbhotell, där information kan lagras och samtidigt göras tillgänglig för andra informationssystem och via internet. S.k. bulletproof hosts, som är en form av värdtjänstbolag, samverkar enligt de brottsbekämpande myndigheterna inte med dem. Det kan till och med vara en del av företagens affärsmodell att inte samverka med myndigheter, vilket gör att Polismyndigheten betraktar företagen som en möjliggörare av crime as a service. Sådana bolag är ett vanligt redskap för kriminella och statsaktörer. Bolagen friskriver sig ofta från det som finns på serverutrymmet de tillhandahåller. De aktörerna är helt avgörande vid brottsbekämpning i cybermiljö. Dessutom avser vissa ingripanden enligt den nya lagen lagrad data. En skyldighet för värdtjänstbolag att lämna upplysningar till de brottsbekämpande myndigheterna skulle enligt Polismyndigheten innebära mycket mindre integritetsintrång för enskilda, eftersom myndigheten då kan rikta sig direkt mot den fysiska eller virtuella server som är målet för ingripandet, utan att påverka eller ta del av annan verksamhet och annan information som inte är relevant. Alternativa former av polisiära ingripanden, t.ex. husrannsakan, är inte kostnadseffektiva varken för myndigheterna eller för värdtjänstbolagen,

eftersom sökande efter relevant server kan medföra nedstängning av verksamhet som inte är illegal och därmed drabba utomstående i större utsträckning.

Det kan konstateras att frågan om en utvidgning av medverkansskyldigheten enligt LEK har diskuterats i olika sammanhang (se bl.a. Lag om elektrisk kommunikation m.m., prop. 2002/03:110, s. 121 f., Genomförande av direktivet om inrättande av europeisk kodex för elektronisk kommunikation, prop. 2021/22:136, s. 127 f. och SOU 2023:22 s. 355 f.). Frågan om utvidgad medverkansskyldighet ligger utanför utredningens direktiv och är enligt utredningens mening alltför komplex för att rymmas inom ramen för utredningen.

Det skulle emellertid kunna diskuteras om de som ansvarar för de nu aktuella tjänsterna skulle kunna åläggas en mer begränsad skyldighet, som enbart består i att lämna de upplysningar som den ingripande myndigheten behöver för att kunna lokalisera en viss server. Inte heller den frågan ryms inom utredningens ram.

18.5 När beslut ska upphävas

Utredningens förslag

Om det inte längre finns skäl för ett beslut om ingripande enligt den nya lagen ska den ingripande myndigheten omedelbart upphäva beslutet. Det gäller dock inte åklagares beslut i fråga om radering som har genomförts.

Skälen för utredningens förslag

Enskilda bör givetvis inte utsättas för integritetsintrång längre än vad som är nödvändigt med hänsyn till ändamålet med ingripandet. Ju längre tid som går mellan beslutet om ett ingripande och att det verkställs, desto större är risken att förhållandena ändras så att beslutet inte längre framstår som motiverat. Det gäller särskilt i cybermiljö där förhållandena kan ändras mycket snabbt.

Om förutsättningarna för beslutet har förändrats, så att det inte längre finns skäl för ingripandet ska beslutet upphävas. Så kan vara fallet såväl innan ingripandet har hunnit genomföras som under genomförandet. En påbörjad radering som inte i sin helhet har genom-

förts ska då upphöra. Även i fråga om ändring och blockering innebär det att åtgärden ska upphöra. Det kan exempelvis visa sig att det misstänkta brottet redan har hunnit fullbordas eller att den brottsliga verksamheten har upphört. Upphävande kan även aktualiseras om den brottsliga verksamheten visade sig vara av mindre allvarlig art, vilket kan innebära att skälen för beslutet har fallit bort. Det kan även visa sig att informationssystemet som åtgärden riktar sig mot inte längre är åtkomligt eller att det har uppstått oförutsedda tekniska hinder mot att genomföra ingripandet. Ett beslut om ingripande kan även behöva upphävas till viss del, t.ex. därför att en viss åtgärd inte aktualiseras. Ett beslut om ingripande bör också upphävas om det efter beslutet visar sig att det riktar sig mot ett informationssystem eller uppgifter i ett informationssystem som omfattas av förbud enligt den nya lagen (se avsnitt 15.2), eftersom åtgärden då inte är tillåten. Om ingripandet avser även andra informationssystem eller uppgifter som inte omfattas av förbud får ingripandet i övriga delar fortsätta.

Utredningen ser det som en naturlig del av återrapporteringen till en beslutsfattare inom samma myndighet att ange hur ingripandet har genomförts. Vid en sådan återrapportering bör beslutsfattaren, om ändamålet med ingripandet har uppnåtts i sin helhet, avsluta ärendet med ett beslut. På så sätt tydliggörs att något nytt intrång i informationssystemet inte är tillåtet.

När det gäller blockering kan det dock, som tidigare nämnts, finnas skäl för ett nytt beslut när tiden för den ursprungliga blockeringen löper ut. Det får då bedömas om förutsättningarna för ingripande enligt lagen alltjämt är uppfyllda.

Det bör ankomma på den ingripande myndigheten, dvs. Polismyndigheten, Säkerhetspolisen eller Tullverket, att upphäva ett beslut om ingripande. Även när det gäller beslut om radering som har fattats av åklagare anser utredningen att skyldigheten att upphäva beslutet bör vila på Polismyndigheten, Säkerhetspolisen respektive Tullverket. Skälet till det är att den ingripande myndigheten har bäst förutsättningar att bedöma när det inte längre finns behov av ett ingripande.

Det som har sagts om upphävande av beslut bör dock inte gälla ett åklagarbeslut om radering som hunnit genomföras i sin helhet. En sådan åtgärd kan nämligen inte ändras genom ett efterkommande beslut.

19 Rättssäkerhetsgarantier

19.1 Underrättelser

19.1.1 Allmänt om behovet av underrättelse till enskilda

Utredningens bedömning

Det finns inget generellt behov av att underrätta enskilda vilkas uppgifter har varit föremål för ingripanden enligt den nya lagen.

Skälen för utredningens bedömning

Underrättelse till enskild som en rättssäkerhetsgaranti

Europakonventionen ställer inga särskilda krav på att en enskild som utsatts för ingripanden från brottsbekämpande myndigheter i syfte att förhindra eller avbryta brott ska underrättas om det. Det kan emellertid ha betydelse för rätten till en rättvis rättegång enligt artikel 6 i konventionen.

Som utredningen tidigare anfört (se avsnitt 12.4) kan ingripanden i cybermiljö i vissa fall leda till intrång som för den enskilde har likheter med de intrång som användning av tvångsmedel, bl.a. husrannsakan och genomsökning på distans men även hemliga tvångsmedel, kan medföra. Hur stort intrånget blir i det enskilda fallet beror bl.a. på vilken typ av åtgärd som ingripandet avser, vilka uppgifter som åtgärden riktar sig mot och villkoren för ingripandet. Ingripanden i cybermiljö riktas, i motsats till det som gäller för t.ex. hemlig dataavläsning, inte mot personer utan mot informationssystem. Indirekt kommer dock ett sådant ingripande att beröra den som äger eller använder informationssystemet.

Europadomstolen har slagit fast att som huvudregel ska den som har varit föremål för ett hemligt tvångsmedel underrättas om det i efterhand. Annars berövas han eller hon möjligheten att få en prövning angående lagligheten av tvångsmedlet. Domstolen har dock inte ens i de fallen ställt något absolut krav på underrättelse, eftersom en underrättelse kan äventyra syftet med åtgärden och avslöja hemliga arbetsmetoder inom den brottsbekämpande myndigheten. Att de berörda inte i efterhand blir informerade kan inte i sig innebära att den hemliga tvångsåtgärden inte var nödvändig i ett demokratiskt samhälle enligt artikel 8 i Europakonventionen. Däremot får det enligt domstolen inte innebära att den berörda personen i praktiken berövas sin möjlighet att söka gottgörelse för olagliga övervakningsåtgärder. En underrättelse bör därför lämnas så snart syftet med begränsningen inte längre äventyras (Europadomstolens domar den 6 september 1978 i Klass m.fl. mot Tyskland, nr 5029/71, punkten 58, den 29 juni 2006 i Weber och Saravia mot Tyskland, nr 54934/00, punkten 136, den 18 augusti 2009 i Kennedy mot Förenade Kungariket, nr 26839/05, punkten 167, den 30 januari 2008 i Association for European Integration and Human Rights och Ekimdzhiev mot Bulgarien, nr 62540/00, punkterna 90 och 91 och den 4 december 2015 i Roman Zakharov mot Ryssland, nr 47143/06, punkterna 286–288).

I förarbetena till lagstiftning om hemliga tvångsmedel har en skyldighet att underrätta berörda personer om att hemliga tvångsmedel har använts även ansetts kunna ha en återhållande verkan på användningen av hemliga tvångsmedel och bidra till att prövningen inför ett beslut görs på ett än mer noggrant sätt (prop. 2006/07:133 s. 30). En sådan skyldighet kan också bidra till en mer effektiv tillsyn och vara till fördel vid en framtida utvärdering av lagstiftningen (prop. 2022/23:126 s. 81 och SOU 2025:109 s. 209 f.).

Underrättelse till enskilda om användning av hemliga tvångsmedel regleras framför allt i 27 kap. 31–33 §§ RB, 16–18 §§ preventivlagen och 28 och 29 §§ lagen om hemlig dataavläsning. Undantag från kravet på underrättelse gäller bl.a. vid viss sekretess och i de fall där integritetsintrånget kan antas vara ringa eller om en enskild redan har fått del av eller tillgång till uppgifterna som ska ingå i en underrättelse. Någon underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse (27 kap. 31 § tredje och femte styckena RB). Vid sådana brott som hör till

Säkerhetspolisens verksamhetsområde finns det i dag ingen underrättelseskyldighet.

Syftet med underrättelser till enskilda

Generellt sett bedrivs underrättelseverksamhet och brottsutredningar under sekretess. Det innebär att den som är föremål för de brottsbekämpande myndigheternas intresse normalt inte informeras om det innan insynsrätten för den som är skäligen misstänkt aktualiseras. Vissa typer av åtgärder som en enskild kan utsättas för i den brottsbekämpande verksamheten är av den arten att han eller hon behöver underrättas om dem för att kunna ta tillvara sin rätt. Det gäller såväl de som är misstänkta för brott som andra som kan beröras av bl.a. brottsutredningar. Andra åtgärder, framför allt sådana som görs öppet eller som direkt riktas mot en person som är närvarande vid verkställigheten, kräver inte någon underrättelse. Det finns bestämmelser om viss underrättelseskyldighet även i polisens ordningshållande verksamhet, se t.ex. 15 § första stycket polislagen.

För vissa straffprocessuella tvångsmedel finns det föreskrifter i bl.a. RB om att den verkställande myndigheten ska underrätta den berörde i efterhand i de fall där han eller hon inte var närvarande vid verkställigheten. Även beträffande hemliga tvångsmedel finns det bestämmelser bl.a. i RB om att den berörde ska underrättas i efterhand. Det finns emellertid i sistnämnda fall betydande undantag från underrättelseskyldigheten. Någon underrättelse behöver framför allt inte lämnas om sekretess hindrar det. Vid andra polisära åtgärder finns det inte något generellt krav på att den som har utsatts för åtgärden ska underrättas om den.

Inget generellt behov av underrättelser

Även om ingripanden i cybermiljö och hemliga tvångsmedel i vissa avseenden kan vara jämförbara med varandra när det gäller intrång i den personliga integriteten, finns det även väsentliga skillnader.

En viktig skillnad är att ingripanden i cybermiljö normalt inte äger rum i hemlighet. Tvärtom kommer det i många fall att ligga i den ingripande myndighetens intresse att vara öppen och tydlig med att ingripandet görs. Som exempel kan nämnas att en webbplats där narko-

tika säljs eller där brottsuppdrag ”utannonseras” stängs ner. Då kan polisen t.ex. informera om nedstängningen på webbplatsen. Det är en metod som brukar användas i andra länder. Ett annat exempel är att pågående bedrägerier mot investerare hindras genom att meddelanden till en viss tjänst blockeras och att den brottsbekämpande myndigheten informerar om sitt ingripande på det sätt som nyss nämnts. När polisen anmodar systemägare att göra visst material oåtkomligt kommer åtgärden likaså att utföras öppet, men den vidtas då av systemägaren själv. I stor utsträckning kan det alltså förutsättas att den som blir föremål för ett ingripande enligt den nya lagen snabbt får kännedom om det. Om ingripandet resulterar i en förundersökning kommer den som blir misstänkt eller som annars förhörs i utredningen likaså att få information om ingripandet. Det finns därför inget generellt behov av att underrätta den vars informationssystem eller uppgifter har varit föremål för ett ingripande.

Även om den eller de som använder de informationssystem som har varit föremål för ingripanden inte får någon formell underrättelse kommer de alltså i de flesta fall att bli medvetna om att en åtgärd har vidtagits. Det kan t.ex. handla om att, i de fall där den ingripande myndigheten har ändrat lösenordet till ett informationssystem för att bereda sig tillgång till uppgifter i det, ett meddelande automatiskt skickas till den enskilde om att lösenordet har ändrats. Likaså kommer som regel en eventuell kryptering av informationssystem att snabbt upptäckas av den som använder systemet.

När det gäller andra åtgärder enligt den nya lagen än radering är de flesta åtgärder, som tidigare nämnts, tillfälliga och kortvariga. Det innebär att den eller de som använder det informationssystem som ingripandet riktar sig mot kommer att få kännedom om det så snart det genomförs, t.ex. genom att uppgifterna inte längre är åtkomliga eller att informationssystemet inte fungerar som vanligt. I sådana fall skulle en underrättelse inte ha någon funktion att fylla. En generell underrättelseskyldighet skulle däremot kräva omfattande resurser hos de brottsbekämpande myndigheterna för att administrera underrättelserna. Det gäller särskilt om ingripandet rör delar av större informationssystem som används av flera personer.

Det förhåller sig annorlunda med ett ingripande som syftar till att kartlägga om det förekommer eller har förekommit kommunikation mellan informationssystem som kan antas utnyttjas i brottslig verksamhet. Sådana ingripanden kan som utgångspunkt inte upptäckas

av den som använder informationssystemet. I det fallet skulle emellertid ingripandena förlora sitt syfte om den enskilde skulle underrättas om dem. En underrättelse bör därmed inte heller i de fallen lämnas.

19.1.2 Underrättelse i vissa fall

Utredningens förslag

En enskild, vars uppgifter genom ett ingripande enligt lagen har raderats eller blockerats under längre tid än en månad, ska underrättas om ingripandet så snart det lämpligen kan göras, om inte han eller hon har fått kännedom om ingripandet på annat sätt. Om det inte är känt vem som ska underrättas om ingripandet, och det inte heller finns anledning att anta att denne genom rimliga åtgärder kan identifieras, får underrättelse underlåtas. Någon underrättelse behöver inte heller lämnas om det gäller sekretess enligt 18 kap. 9 § offentlighets- och sekretesslagen.

Den myndighet som har beslutat om ingripandet eller, i fråga om åklagares beslut om radering, har ansökt om åtgärden ansvarar för underrättelsen.

Skälen för utredningens förslag

I några situationer kan det finnas behov av underrättelse

Som framgått av avsnitt 14.5 anser utredningen att det bör ställas särskilda krav på ingripanden i form av radering och att en sådan åtgärd bör omgärdas av särskilda rättssäkerhetsgarantier med hänsyn till att radering är en åtgärd som är oåterkallelig. Mot den bakgrunden anser utredningen att den vars uppgifter har raderats bör underrättas om det. Även om den enskilde som utgångspunkt kommer att upptäcka att uppgifterna i fråga har raderats, kommer han eller hon inte att veta vem eller vilka som ligger bakom raderingen. Genom en underrättelse kommer den enskilde att få veta att det är en myndighet som har vidtagit åtgärden. Utredningen har i avsnitt 16.2.4 funnit att åklagarens beslut om radering inte bör få överklagas eller på annat sätt prövas av någon fristående myndighet. En underrättelse

ger den enskilde möjlighet att söka gottgörelse för en radering som han eller hon anser ha varit olaglig genom att yrka skadestånd av staten. Utredningen återkommer till den frågan i avsnitt 20.3.

En blockering av uppgifter som pågår under en längre tid får, i likhet med radering, anses leda till ett större intrång än övriga ingripanden. Det finns därför enligt utredningen skäl att även underrätta den vars uppgifter har blockerats under en tid som överstiger en månad om åtgärden. Även om den enskilde som utgångspunkt kommer att upptäcka att uppgifterna i fråga har blockerats kommer han eller hon inte att veta vem eller vilka som ligger bakom blockeringen. Genom en underrättelse kommer den enskilde att få veta att åtgärden har vidtagits av en myndighet. På så sätt ges den enskilde möjlighet att söka gottgörelse för en längre blockering som han eller hon anser varit olaglig genom att yrka skadestånd mot staten.

Tidpunkten för underrättelse och vem som bör ansvara för den

En viktig fråga är när underrättelsen ska lämnas. Den bör enligt utredningens mening lämnas så snart det är lämpligt. När det inte längre finns någon risk för att ingripandet äventyras och det inte heller i övrigt finns något hinder mot underrättelse bör alltså den eller de som ska underrättas få ett meddelande om ingripandet. Det bör uttryckas så att en underrättelse ska lämnas så snart det lämpligen kan göras.

Den myndighet som har beslutat om ingripandet eller, i fråga om åklagares beslut om radering, har ansökt om åtgärden bör ansvara för underrättelsen.

Innehållet i underrättelsen

Av underrättelsen bör det åtminstone framgå vilken åtgärd som ingripandet avsåg, vilket informationssystem eller användarkonto eller annan avgränsad del av ett informationssystem som ingripandet riktades mot och när ingripandet gjordes. Som framgått av avsnitt 18.4 bör det i den nya lagen införas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter. Det möjliggör att detaljerna kring underrättelser kan regleras i förordning.

Undantag från underrättelseskyldigheten

Något som är av stor betydelse i sammanhanget är att ingripanden i cybermiljö ofta kommer att äga rum utan att det finns någon identifierbar person som åtgärden riktas mot. Som framgått av avsnitt 13.2 förutsätter ett ingripande enligt den nya lagen inte att det finns någon identifierad person som kan ligga bakom brottet eller den brottsliga verksamheten, utan endast ett identifierat informationssystem. Det är långt ifrån säkert att informationssystemet kan knytas till en fysisk person på det sätt som krävs i en förundersökning. I de fallen är det inte praktiskt möjligt för den brottsbekämpande myndigheten att underrätta någon om den vidtagna åtgärden. Underrättelse bör därför kunna underlåtas.

Även i de situationer där det finns anledning att anta att den enskilde åtminstone teoretiskt skulle kunna identifieras bör underrättelse kunna underlåtas i vissa fall. Det kan t.ex. röra sig om att en identifiering skulle kräva orimliga resurser eller ta alltför lång tid. Att försöka identifiera en person som från utlandet agerar för främmande makts räkning torde i de flesta fall vara utsiktslöst. Detsamma gäller kriminella som aktivt, bl.a. genom användning av anonymiseringsmetoder, försöker undgå att förknippas med brott i cybermiljö.

Vidare bör undantag gälla från underrättelseskyldigheten om det gäller sekretess enligt 18 kap. 9 § offentlighets- och sekretesslagen (2009:400). Sekretessen i den bestämmelsen skyddar bl.a. kod, chiffer och liknande (se avsnitt 20.4.1). Sekretessen gäller om det kan antas att syftet med metoden motverkas om uppgiften röjs. De tekniska metoder som de brottsbekämpande myndigheterna använder för att bereda sig tillgång till informationssystem och de hjälpmedel som myndigheterna utvecklar för att kunna tillämpa lagen kan i vissa fall skyddas av den sekretessen. Om så är fallet behöver någon underrättelse inte lämnas.

19.1.3 Underrättelse till en tillsynsmyndighet i stället

Utredningens bedömning

Det bör inte införas någon skyldighet för ingripande myndigheter att underrätta en tillsynsmyndighet om alla beslut om ingripanden enligt lagen.

Skälen för utredningens bedömning

I inhämtningslagen, som reglerar ett hemligt tvångsmedel, finns det ingen motsvarighet till RB:s och preventivlagens krav på underrättelse till enskild. I stället ska Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd underrättas om alla beslut om inhämtning. En sådan underrättelse ska lämnas senast en månad efter det att ärendet om inhämtning avslutades (5 § inhämtningslagen). Frågan om ett krav på underrättelse till enskild borde införas övervägdes när inhämtningslagen infördes. Regeringen uttalade då att en skyldighet att underrätta enskilda om inhämtning av uppgifter i underrättelseverksamhet, skulle riskera att motverka huvudsyftet med underrättelseverksamheten, med hänsyn till verksamhetens framåtblickande perspektiv och övergripande natur. En sådan skyldighet skulle enligt regeringen därför behöva förses med en rad undantag och det skulle i många fall kunna ta lång tid innan en underrättelse skulle kunna lämnas. Den eventuella identifiering och granskning av kommunikationen som måste föregå en underrättelse skulle dessutom kunna innebära ett ytterligare integritetsintrång (prop. 2011/12:55 s. 107).

Vid användning av hemliga tvångsmedel enligt lagen (2022:700) om särskild kontroll av vissa utlänningar gäller inte heller någon underrättelseskyldighet. Det motiveras av starka sekretesskäl, eftersom lagen rör terroristbrott, som är riktade mot statens centrala och vitala intressen och tillhör Säkerhetspolisens verksamhetsområde (prop. 2018/19:86 s. 83). I det fallet finns det inte heller någon skyldighet att underrätta tillsynsmyndigheten.

Utredningen anser att det inte bör införas någon generell skyldighet för ingripande myndigheter att underrätta en tillsynsmyndighet om alla beslut om ingripanden enligt den nya lagen.

19.1.4 Underrättelse om ett felaktigt beslut om radering

Utredningens förslag

Har ett interimistiskt beslut om radering redan hunnit genomföras när åklagaren prövar frågan, ska åklagaren, i stället för att upphäva beslutet, underrätta Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd om det interimistiska beslutet och sitt ställningstagande.

Åklagaren ska underrätta den vars uppgifter har raderats, om han eller hon är känd, om sitt ställningstagande och, om det finns en kopia av de uppgifter som har raderats, om möjligheten att begära en kopia från den ingripande myndigheten.

Skälen för utredningens förslag

Underrättelse till Säkerhets- och integritetsskyddsnämnden

I avsnitt 16.2.3 har utredningen föreslagit att en åklagare, när han eller hon underrättas om ett interimistiskt beslut om radering, så snart som möjligt ska pröva beslutet. Om åklagaren bedömer att det saknas grund för beslutet, ska han eller hon upphäva det. Det gäller även ett beslut om tillträde som är knutet till ingripandebeslutet.

I vissa fall kan det, som framgått av avsnitt 16.2.2, krävas att radering genomförs mycket snabbt. Det kan ibland vara det enda sättet att förhindra eller avbryta ett allvarligt brott. Beroende på mängden uppgifter som ska raderas, bör raderingen normalt kunna avslutas förhållandevis snabbt. Det innebär att ett beslut av åklagare att upphäva ett interimistiskt beslut om radering i många fall skulle sakna faktisk verkan. Om ett interimistiskt beslut om radering redan har hunnit genomföras när åklagaren prövar beslutet finns det ingen möjlighet för åklagaren att vidta någon åtgärd, utöver prövningen om det finns grund för åtgärden. De eventuella negativa konsekvenser för den vars informationssystem har varit föremål för ingripandet kan således inte läkas i efterhand. En lämplig lösning kan då vara att underrätta ett tillsynsorgan, som har möjlighet att undersöka om handläggningen har varit lagenlig. Det är en typ av rättssäkerhetsgaranti som finns beträffande viss brottsbekämpande verksamhet, bl.a. handläggning av hemliga tvångsmedel. En sådan ordning ger den

enskilde bättre möjlighet att bedöma om det finns skäl för att yrka skadestånd om han eller hon anser att beslutet har fattats på felaktiga grunder. Utredningen anser, vilket utvecklas närmare i avsnitt 19.3, att särskild tillsyn bör utövas över den nya lagen och att den ska utövas av Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd. Åklagaren bör därför underrätta tillsynsmyndigheten om besluten i fråga.

Av underrättelsen bör det framgå vilket interimistiskt beslut som har fattats, i vilket informationssystem, eller användarkonto eller annan avgränsad del av ett informationssystem, som ingripandet gjordes, när ingripandet gjordes, och åklagarens ställningstagande. Som framgått av avsnitt 18.4 bör det i den nya lagen införas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter. Det möjliggör att detaljerna beträffande underrättelse kan regleras i förordning.

Som framgått av avsnitt 16.2.3 bör, om möjligt, en kopia av de uppgifter som har raderats bevaras under viss tid för att tillsynsorganet ska kunna ta del av kopian. Eftersom tillsynsorganet självständigt avgör i vilka fall och på vilket sätt tillsyn ska utövas är syftet med regleringen inte att sådana kopior ska överlämnas till tillsynsorganet annat än på tillsynsorganets uttryckliga begäran.

Underrättelse till enskild om möjligheten att få en kopia

I all mänsklig verksamhet kan fel begås. Om det är möjligt att på ett enkelt sätt rätta till ett fel som har begåtts av någon i en myndighet och som kan ha drabbat en enskild är det angeläget att det görs, för att bevara tilltron till myndigheter. Om den ingripande myndigheten har tillgång till en kopia av det som har raderats bör den därför göras tillgänglig för den berörde, om han eller hon är intresserad av det. Utöver att underrätta Säkerhets- och integritetsskyddsnämnden om att åklagaren anser att en felaktig radering har genomförts bör den, vars uppgifter har raderats, ges möjlighet att begära hos den ingripande myndigheten att få en kopia av det som har raderats och uppgift om åklagarens ställningstagande. Det bör ligga på åklagaren att underrätta honom eller henne om det, under förutsättning att personen är känd. Det bör i så fall framgå av anmälan av det interimistiska beslutet om radering. Åklagaren bör alltså inte ha någon skyldighet

att eftersöka personen i fråga. Uppgiften att se till att en kopia lämnas ut bör ligga på den ingripande myndigheten, även om åklagaren skulle ha tillgång till en kopia.

Det bör framhållas att den som har utsatts för en myndighetsåtgärd långt ifrån alltid vill ha någon kontakt med myndigheten i fråga. Det är t.ex. inte ovanligt att beslag som ska lämnas tillbaka inte alltid hämtas ut. Det bör därför ankomma på den enskilde att själv ta ställning till om han eller hon vill ha den erbjudna kopian.

19.2 Dokumentation

Utredningens förslag

Beslut och åtgärder enligt den nya lagen ska dokumenteras.

Skälen för utredningens förslag

Allmänt om dokumentationsskyldighet

Krav på dokumentation i det allmännas verksamhet är ett viktigt inslag i regleringen av myndigheternas verksamhet, som bl.a. syftar till att säkerställa en god förvaltning och att trygga den enskildes rättssäkerhet. Att beslut och andra åtgärder dokumenteras kan motverka godtycklig maktutövning och bidra till att säkerställa krav på omsorgsfull handläggning och enhetlig bedömning. Dokumentation är av särskild vikt när det handlar om åtgärder som avses få faktiska verkningar för en person i det enskilda fallet.

I den brottsbekämpande verksamheten finns det en mängd regler som styr hur myndigheterna ska gå till väga, bl.a. vilka åtgärder som ska vidtas under olika skeden av handläggning och vilka uppgifter som ska dokumenteras. Dokumentation är en förutsättning för att enskildas rätt till insyn i ett ärende, den s.k. partsinsynen, ska kunna tillgodoses. Om det finns material i ett ärende som visar vad som har hänt i ärendet stärker det den enskildes möjlighet till efterhandskontroll. Partsinsynen hör samman med kravet på en rättvis rättegång enligt artikel 6 i Europakonventionen. Uttrycket rättvis rättegång täcker hela det straffrättsliga förfarandet och är alltså inte begränsat till rättegången i domstol men särregleras i de förfaranden som före-

går lagföring. En bestämmelse om rättvis rättegång finns också i 2 kap. 11 § RF. Kravet på dokumentation skapar även underlag för offentlig insyn och kontroll (Stärkt skydd för polisanställda, prop. 2023/ 24:102, s. 10 f.).

Som tidigare nämnts gäller inte förvaltningslagen i brottsbekämpande verksamhet. Bestämmelser om krav på dokumentation i förundersökning finns för Polismyndigheten, Säkerhetspolisen, Tullverket och åklagare i framför allt RB och förundersökningskungörelsen (1947:948). Både polislagen och tullbefogenhetslagen innehåller också bestämmelser om dokumentationsskyldighet vid olika typer av ingripanden mot enskilda (se bl.a. 27 och 28 §§ polislagen och 7 kap. 6 § tullbefogenhetslagen).

Det finns även bestämmelser om dokumentationsskyldighet när det gäller preventiva tvångsmedel (19 § preventivlagen och 8 § inhämtningslagen). Skälet till att de bestämmelserna infördes var bl.a. att det förekom brister i dokumentationen när det inte fanns någon lagstadgad dokumentationsskyldighet och att Europadomstolen kräver att åtgärder vid användning av hemliga tvångsmedel ska dokumenteras, för att tillsynsorgan senare ska kunna genomföra erforderlig tillsyn (se bl.a. Rättssäkerhetsgarantier och hemliga tvångsmedel, SOU 2018:61 s. 82 och prop. 2023/24:117 s. 81).

Det bör ställas krav på dokumentation av ingripandena

Eftersom den nya lagen inte syftar till att utreda och lagföra brott enligt RB och inte heller avser de former av ingripanden som ska dokumenteras enligt polislagen, tullbefogenhetslagen eller andra särskilda lagar, behövs det en bestämmelse om dokumentationsskyldighet i den nya lagen. Den bör omfatta både beslut och andra åtgärder enligt lagen. Dokumentationsskyldigheten behövs för att kunna säkerställa enskildas insyn och skapa goda förutsättningar för tillsyn över att regleringen efterlevs.

Uppgifterna bör dokumenteras så att det är möjligt att på ett överskådligt sätt följa beslut om ingripanden i cybermiljö och hur de genomförs.

Med hänsyn till att det kan variera över tid vilka uppgifter som behöver dokumenteras med tanke på bl.a. teknikutvecklingen, anser utredningen att en detaljerad lista på åtgärder som ska dokumenteras

inte är ändamålsenlig (jfr bl.a. prop. 2022/23:126 s. 181 f.). Exempel på uppgifter som regelmässigt bör dokumenteras – utöver innehållet i besluten – är vem som har beslutat om ingripande, när beslutet fattades och om det har ändrats eller upphävts. Även vilka uppgifter som ingripandet har omfattat och om uppgifter har förstörts därför att de omfattas av förbud mot ingripande bör dokumenteras. Detsamma gäller resultatet av genomförandet, t.ex. att myndigheten visserligen har lyckats bereda sig tillgång till ett informationssystem men inte kunnat vidta någon ytterligare åtgärd. Vidare bör tidpunkten för ingripandet dokumenteras (jfr prop. 2022/23:126 s. 225). Skyldigheten att dokumentera bör gälla både för den som beslutar, såvitt gäller uppgifter som inte framgår av beslutet, och i övrigt för den som genomfört ingripandet.

Det är angeläget att dokumentationen görs på ett sätt som inte riskerar att röja källor vad gäller sådana uppgifter som omfattas av förbud mot ingripanden.

19.3 Tillsyn

19.3.1 Särskild tillsyn behövs

Utredningens bedömning

Den nya lagstiftningen kan innebära sådana integritetsrisker att det behövs särskild tillsyn.

Skälen för utredningens bedömning

Extraordinär tillsyn

Tillsynen över brottsbekämpande myndigheter bedrivs antingen som ordinarie eller extraordinär tillsyn. Den tillsyn som bedrivs av Riksdagens ombudsmän (JO) och Justitiekanslern anses vara extraordinär tillsyn.

JO ska utöva tillsyn över att bl.a. statliga myndigheter och tjänstemän och andra befattningshavare vid sådana myndigheter följer lagar och andra författningar och i övrigt fullgör sina åligganden (11, 12 och 14 §§ lagen [2023:499] med instruktion för Riksdagens om-

budsmän). JO ska särskilt se till att myndigheter och tjänstemän följer RF:s föreskrifter om saklighet och opartiskhet och att det inte görs intrång i enskildas grundläggande fri- och rättigheter i den offentliga verksamheten (12 § första stycket lagen med instruktion för Riksdagens ombudsmän). Tillsynen bedrivs genom prövning av klagomål från allmänheten och genom inspektioner och andra undersökningar (17 § lagen med instruktion för Riksdagens ombudsmän). En ombudsman får genom beslut i ett ärende uttala sig om huruvida en åtgärd av någon som står under ombudsmännens tillsyn strider mot en lag eller någon annan författning eller annars är felaktig eller olämplig. En ombudsman får även göra uttalanden för att främja en enhetlig och ändamålsenlig rättstillämpning (20 § lagen med instruktion för Riksdagens ombudsmän). Vidare får en ombudsman som särskild åklagare väcka åtal mot en befattningshavare som genom att åsidosätta vad som åligger honom eller henne i tjänsten eller uppdraget har begått annan brottslig gärning än tryckfrihetsbrott eller yttrandefrihetsbrott (21 § lagen med instruktion för Riksdagens ombudsmän).

Justitiekanslern har också tillsyn över att bl.a. statliga myndigheter och tjänstemän och andra befattningshavare vid sådana myndigheter följer lagar och andra författningar samt i övrigt fullgör sina åligganden (1 och 2 §§ lagen [1975:1339] om Justitiekanslerns tillsyn). Justitiekanslern får som särskild åklagare väcka åtal mot en befattningshavare som har begått brottslig gärning genom att åsidosätta vad som åligger honom i tjänsten eller uppdraget (5 § lagen om Justitiekanslerns tillsyn). Justitiekanslern kan också göra anmälan om bl.a. disciplinära påföljder, avskedande eller avstängning av befattningshavare som har åsidosatt vad som åligger honom eller henne i tjänsten (6 § lagen om Justitiekanslerns tillsyn). Justitiekanslern ansvarar vidare för statens frivilliga skadereglering. Anspråk på ersättning handläggs enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten.

Tillsyn över vissa områden inom brottsbekämpningen

Vissa myndigheter, som har som en reguljär arbetsuppgift att utöva tillsyn över ett visst utpekat regelverk, utövar ordinarie tillsyn.

Den tillsyn som bedrivs inom åklagarväsendet har sin grund i regleringen i 7 kap. RB och åklagarverksamhetens hierarkiska uppbyggnad. Enligt 7 kap. 5 § RB får riksåklagaren, överåklagare och vice överåklagare överta uppgifter som ska utföras av lägre åklagare. De åklagarna har, enligt 7 kap. 2 § RB, var och en inom sitt verksamhetsområde ansvaret för åklagarverksamheten. Tillsynen är generell, dvs. omfattar hela åklagarverksamheten.

Inom Åklagarmyndigheten bedrivs tillsynen bl.a. av riksåklagaren, som ska verka för lagenlighet, följdriktighet och enhetlighet vid åklagarnas rättstillämpning (3 § förordningen [2015:743] med instruktion för Åklagarmyndigheten). Vid myndigheten finns det dels en funktion som biträder riksåklagaren i hans eller hennes åklagaruppgifter, dels utvecklingscentrum som inom särskilda ansvarsområden ansvarar för tillsyn över åklagare och rättslig utveckling av åklagarverksamheten (17 § förordningen med instruktion för Åklagarmyndigheten).

Integritetsskyddsmyndighetens (IMY) uppgift är att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter och att underlätta det fria flödet av sådana uppgifter inom EU. IMY är tillsynsmyndighet enligt brottsdatalagen (2018:1177). Det innebär att IMY har tillsyn över myndigheters personuppgiftsbehandling vid brottsbekämpning, lagföring och verkställighet av påföljder inom hela rättskedjan.

Säkerhets- och integritetsskyddsnämnden inrättades år 2008 som en förvaltningsmyndighet under regeringen. Myndigheten leddes av nämnden fram till den 1 mars 2026, då den bytte namn till Myndigheten för säkerhet och integritetsskydd och fick ändrad ledningsform genom att den blev en s.k. enrådighetsmyndighet (Budgetpropositionen för 2026, prop. 2025/26:1, Utgiftsområde 4, s. 100 f.). Säkerhets- och integritetsskyddsnämnden är numera ett självständigt beslutsorgan inom myndigheten, men har oförändrat uppdrag. Nämnden har tillsyn bl.a. över brottsbekämpande myndigheters användning av hemliga tvångsmedel. Nämndens tillsyn beskrivs närmare i avsnitt 19.3.2.

Det förekommer även annan tillsyn över brottsbekämpande myndigheters verksamhet, t.ex. tillsyn över tillämpningen av säkerhetsskyddslagen (2018:585). Sådan tillsyn saknar dock betydelse i detta sammanhang.

Ingripanden enligt den nya lagen bör vara föremål för särskild tillsyn

En grundläggande fråga är om tillämpningen av den nya lagen bör vara föremål för särskild tillsyn eller om det är tillräckligt med den extraordinära tillsyn som utförs av JO och Justitiekanslern och den interna kontroll som förekommer i de myndigheter som ska tillämpa lagen.

Det som talar för att den nya lagstiftningen bör bli föremål för särskild tillsyn är framför allt att det handlar om ingripanden som i vissa fall kan medföra samma typ av kränkningar av enskildas personliga integritet som bl.a. vissa tvångsmedel. Det förhållandet att ingripanden enligt den nya lagen i betydande utsträckning förväntas äga rum öppet innebär att den som använder ett informationssystem visserligen kommer att märka att någon har vidtagit någon åtgärd med det, men det är inte självklart att han eller hon förstår att det är en brottsbekämpande myndighet som har gjort ett ingripande.

Den digitala miljön innehåller numera allt fler känsliga uppgifter om de flesta personer. Även om det kan hävdas att det är ett fritt val att hantera sådana uppgifter i den digitala miljön kan konstateras att det numera för de allra flesta kan vara svårt att avstå från att t.ex. sköta sina ekonomiska transaktioner och att hantera hälsoinformation och annan känslig personlig information i ett digitalt medium. Det kan också vara svårt för enskilda att förstå vad användning av modern teknik kan få för konsekvenser för den personliga integriteten. Det kan leda till misstro mot brottsbekämpande myndigheter om en lagstiftning av det nu aktuella slaget införs utan att det finns goda rättssäkerhetsgarantier för enskilda. En effektiv tillsyn är då en viktig faktor, vilket talar för att det behövs särskild tillsyn.

Ett annat skäl till att det bör införas särskild tillsyn är att det är fråga om en ny lagstiftning inom ett område som till stor del är oreglerat. Dessutom har utredningen föreslagit att lagen ska vara tidsbegränsad. Förekomsten av tillsyn kan då spela en viktig roll för att belysa om lagstiftningen har använts på det avsedda sättet och har

haft den nytta som förväntats. Det är frågor av avgörande betydelse inför överväganden om lagen bör permanentas.

Det som främst talar mot att införa särskild tillsyn är att de flesta polisiära metoder inte är underkastade särskild tillsyn. Det gäller även så ingripande åtgärder som frihetsberövanden. Behovet av särskild tillsyn över polisen är emellertid något som har diskuterats och varit föremål för överväganden i ett flertal utredningar (se bl.a. Förstärkt granskning av polis och åklagare, SOU 2003:41, Tillsyn över polisen, SOU 2013:42, och Tillsyn över polisen och Kriminalvården, SOU 2015:57). De flesta polisiära ingripanden görs öppet. Som tidigare nämnts kan det tala för att det inte behövs någon särskild tillsyn över den nya lagen, men det är inte självklart att det alltid framgår att ingripandet har gjorts av en brottsbekämpande myndighet. I avsnitt 19.1.1 har utredningen redovisat varför det inte heller är givet att den som använder ett visst informationssystem kan eller bör underrättas om att det gjorts ett ingripande i systemet. Det innebär att det, trots att ett ingripande görs öppet, inte kan garanteras att den som har varit utsatt för ingripandet får kännedom om det.

Utredningen anser sammantaget att ingripanden i cybermiljö är en typ av ingripanden som bör omgärdas av särskilda rättssäkerhetsgarantier och att särskild tillsyn därför bör införas. Att enbart förlita sig på den extraordinära tillsyn som utövas av JO och Justitiekanslern och den interna kontrollen i myndigheterna är enligt utredningens mening inte tillräckligt.

19.3.2 Vem som bör utöva tillsynen

Utredningens förslag

Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd ska utöva tillsyn över tillämpningen av den nya lagen.

I lagen om tillsyn över viss brottsbekämpande verksamhet ska det föreskrivas att Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över brottsbekämpande myndigheters tillämpning av lagen om ingripanden i cybermiljö. Tillsynen ska särskilt syfta till att säkerställa att sådan verksamhet bedrivs i enlighet med lag eller annan författning.

Skälen för utredningens förslag

Säkerhets- och integritetsskyddsnämndens nuvarande tillsyn

Säkerhets- och integritetskyddsnämndens uppgift är att utöva tillsyn enligt 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet över bl.a.

1. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter,
2. brottsbekämpande myndigheters användning av andra tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott än de som avses i 1, om inte den som åtgärden utförts hos eller annars riktats mot har närvarat vid åtgärden,
3. Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar, och
4. därmed sammanhängande verksamhet.[1]

Tillsynen utövas genom inspektioner och andra undersökningar. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps (2 § lagen om tillsyn över viss brottsbekämpande verksamhet).

Nämnden är enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet skyldig att på begäran av en enskild kontrollera om han eller hon

1. har utsatts för sådana tvångsmedel som avses i 1 § första stycket lagen om tillsyn över viss brottsbekämpande verksamhet och om användningen av dem och verksamhet som hänger samman med dem har varit i enlighet med lag eller annan författning, eller
2. varit föremål för sådan personuppgiftsbehandling som avses i 1 § andra stycket lagen om tillsyn över viss brottsbekämpande verksamhet och om den har utförts i enlighet med lag eller annan författning.

[1] I prop. 2025/26:147 föreslås att ytterligare en punkt ska läggas till i detta stycke.

Nämnden ska underrätta den enskilde om att kontrollen har utförts. Nämnden får vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad.

Om nämnden i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten eller någon annan behörig myndighet (12 § första stycket förordningen [2025:1484] med instruktion för Myndigheten för säkerhet och integritetsskydd). Om nämnden vid tillsynen uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person, får nämnden anmäla det till Justitiekanslern. Om nämnden uppmärksammar sådana felaktigheter vid kontroll enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet, ska nämnden anmäla det till Justitiekanslern.

Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och upplysningar, den information och det biträde som nämnden begär. Även domstolar och förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter som den begär (4 § lagen om tillsyn över viss brottsbekämpande verksamhet).

Nämndens avgöranden får inte överklagas (6 § lagen om tillsyn över viss brottsbekämpande verksamhet).

Säkerhets- och integritetsskyddsnämnden bör utöva tillsyn

Den första frågan är vilken myndighet som bör ges uppgiften att utöva tillsyn över den nya lagen. Enligt utredningens mening föreslås åklagare ha en så begränsad roll i den nya lagstiftningen att tillsyn inom åklagarväsendet inte skulle tillgodose behovet av tillsyn. IMY har visserligen tillsyn över de brottsbekämpande myndigheter som ska tillämpa den nya lagen, men IMY:s tillsyn avser enbart myndigheternas personuppgiftsbehandling. Det är inte något som står i fokus för den nya lagen, även om viss personuppgiftsbehandling kan aktualiseras. Inte heller IMY skulle därmed vara en lämplig tillsynsmyndighet.

Säkerhets- och integritetsskyddsnämnden utövar redan i dag viss tillsyn över de myndigheter som ska tillämpa den nya lagen. Den tillsynen avser emellertid inte polisiära ingripanden eller arbetsmetoder utan är inriktad på rättslig tillsyn över framför allt beslut och verk-

ställighet av hemliga tvångsmedel och polisens personuppgiftsbehandling. Det bör emellertid framhållas att nämnden även har andra tillsynsuppgifter. Det gäller bl.a. tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Regeringen har nyligen föreslagit att Säkerhets- och integritetsskyddsnämnden även ska utöva tillsyn över brottsbekämpande myndigheters användning av en europeisk utlämnandeorder för trafikuppgifter eller innehållsdata (prop. 2025/26:147 s. 46 f.). Utfärdandet av en europeisk utlämnandeorder för trafikuppgifter eller innehållsdata har enligt förarbetena visserligen stora likheter med vad som i svensk rätt avses med ett hemligt tvångsmedel, men i det fallet rör det sig om en åtgärd som beslutas med stöd av en EU-förordning.

Det finns enligt utredningens mening vissa faktorer som gör att nämnden framstår som det bästa alternativet, om ett befintligt organ ska ges i uppgift att utöva ordinär tillsyn över den nya lagen. Nämnden har för det första god kunskap om brottsbekämpning i allmänhet och om ingripande åtgärder i digital miljö i synnerhet. I en del avseenden har både hemlig dataavläsning och användningen av europeiska utlämnandeorder avseende trafikdata och innehållsdata likhet med ingripanden i cybermiljö. Inte minst genom nämndens mångåriga tillsyn över användning av hemliga och preventiva tvångsmedel har nämnden en god överblick över sådana frågor som kommer att aktualiseras vid tillämpning av den nya lagen. Vidare talar det förhållandet att det bör finnas teknisk expertis på tillsynsmyndigheten, som kan bistå de jurister som ska utöva tillsynen, för att uppgiften bör läggas på nämnden.

Vad bör tillsynen avse?

Eftersom det är fråga om en ny tillsynsuppgift kan det finnas anledning att ange något om vad tillsynen bör avse. Det bör, i likhet med den tillsyn som Säkerhets- och integritetsskyddsnämnden redan bedriver, vara fråga om en rättslig tillsyn över att ingripanden enligt lagen görs i enlighet med lag eller annan författning. Det innebär att tillsynen kan omfatta sådana frågor som om ingripandet har stått i överensstämmelse med tillämpningsområdet för lagen, dvs. om det har funnits tillräcklig anknytning till svenska intressen för att lagen

ska vara tillämplig. Det kan vidare röra sig om förutsättningarna i övrigt för att ingripa enligt lagen har varit uppfyllda, t.ex. om brottet eller brottsligheten har varit av tillräcklig svårhetsgrad eller om det har varit av särskild eller, i fråga om radering, synnerlig vikt att göra ingripandet. Det kan även vara fråga om besluten är korrekt utformade, om dokumentationsskyldigheten har följts eller om genomförandet av ingripandet har varit lagenligt. Det ankommer på Säkerhets- och integritetsskyddsnämnden att bestämma vad tillsynen ska omfatta i det enskilda fallet. I avsnitt 19.1.4 har utredningen föreslagit att nämnden ska underrättas om interimistiska beslut om radering som har hunnit genomföras när åklagaren prövar om det finns skäl för radering. Som tidigare nämnts avgör nämnden självständigt om tillsyn ska utövas och vad den i så fall ska omfatta. Den föreslagna regleringen skiljer sig alltså inte från nuvarande bestämmelser om tillsyn och om underrättelseskyldighet vid användning av hemliga och preventiva tvångsmedel.

Vissa författningsändringar krävs

Nämndens tillsynsområde framgår, som nyss nämnts, av 1 § lagen om tillsyn över viss brottsbekämpande verksamhet där nämndens tillsynsuppgifter räknas upp. För att lagen om polisiära ingripanden i cybermiljö ska omfattas av nämndens tillsynsområde behöver det göras ett tillägg i den paragrafen.

Det bör lämpligen göras genom att föreskriva att nämnden också ska utöva tillsyn över brottsbekämpande myndigheters tillämpning av lagen om polisiära ingripanden i cybermiljö. Det innebär att tillsynen kommer att omfatta inte bara Polismyndighetens, Säkerhetspolisens och Tullverkets tillämpning av lagen utan även åklagarnas. Tillsynen bör särskilt syfta till att säkerställa att ingripanden i cybermiljö görs i enlighet med lag eller annan författning.

Nämndens tillsyn enligt den nya lagen bör utövas på samma sätt som nämndens övriga tillsyn, dvs. genom inspektioner och andra undersökningar. Nämnden bör ha samma möjlighet att uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och att verka för att brister i lag eller annan författning avhjälps som vid annan tillsyn.

Nämnden bör även, om den uppmärksammar förhållanden som kan utgöra brott, anmäla det till Åklagarmyndigheten eller någon annan behörig myndighet. Även möjligheten att anmäla vissa förhållanden till Justitiekanslern bör vara densamma som för den befintliga tillsynen.

En särskild fråga är om nämndens skyldigheter även bör omfatta 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 i enlighet med lag eller annan författning (jfr 3 § lagen om tillsyn över viss brottsbekämpande verksamhet). Någon sådan skyldighet bör enligt utredningens mening inte införas. Den nya lagstiftningen skiljer sig, som tidigare nämnts, från bl.a. hemliga tvångsmedel genom att ingripandena normalt förväntas göras helt öppet. Kontrollmöjligheten enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet har tillkommit som en rättssäkerhetsgaranti, där Säkerhets- och integritetsskyddsnämndens kontroll är avsedd att ersätta enskildas möjlighet att få insyn i sådan brottsbekämpande verksamhet som omgärdas av särskilt stark sekretess. Något motsvarande behov finns inte när det gäller den nya lagen. Någon ändring bör därför inte göras i 3 §. Det sagda innebär att om någon enskild vänder sig till nämnden med ett klagomål över tillämpningen av den nya lagen har nämnden ingen skyldighet att företa några åtgärder. Däremot är det inget som hindrar att ett sådant klagomål, ensamt eller tillsammans med andra uppgifter, kan läggas till grund för ett beslut av nämnden att inleda ett tillsynsärende.

19.4 En tidsbegränsad lag

Utredningens förslag

Den nya lagen ska tidsbegränsas till att gälla i fem år.

Skälen för utredningens förslag

Som utredningen har konstaterat i avsnitt 12.5 behövs nya rättsliga befogenheter för att ingripa mot brott och brottslig verksamhet i cybermiljö. Det kan förväntas att den nya lagen kommer att bli ett effektivt verktyg för att bekämpa brott och brottslig verksamhet i

cybermiljö. Sådan brottslighet har som tidigare nämnts ökat kraftigt under senare år. Behovet av kraftfulla åtgärder mot sådan brottslighet har också uppmärksammats internationellt. De omständigheterna talar för att den nya lagen bör vara permanent.

Det är dock inte möjligt att överblicka hur stort behovet eller nyttan av den nya lagstiftningen är förrän lagen har tillämpats en tid. Det gäller särskilt mot bakgrund av att den snabba tekniska utvecklingen kan väcka frågor om lagen är adekvat utformad i alla delar och om den är tillräcklig för att täcka behoven. Det är faktorer som talar mot att lagen görs permanent.

Mot en permanent lagstiftning kan också anföras att det rör sig om en ny form av polisiära ingripanden, som kan innebära risker för den personliga integriteten. Vidare att ingripanden ska göras i en hittills till största delen oreglerad miljö, vilket likaså kan medföra särskilda risker. Den nya lagen har, vad gäller påverkan på den personliga integriteten, vissa likheter med hemliga tvångsmedel. I stort sett samtliga lagändringar avseende hemliga och preventiva tvångsmedel, som har inneburit att nya tvångsmedel har införts eller har gjort existerande hemliga tvångsmedel tillämpliga på nya områden, har tidsbegränsats. Det har huvudsakligen motiverats med att nya tvångsmedel ger upphov till risker för otillbörliga integritetsintrång (jfr prop. 2019/20:64 s. 100).

Mot den bakgrunden anser utredningen att övervägande skäl talar för att den nya lagen bör tidsbegränsas. Vid en framtida utvärdering kommer nyttan och behovet av den nya lagen återigen att analyseras och bedömas för att ge ytterligare underlag inför ett ställningstagande till om det finns skäl att permanenta lagen.

Det är också fråga om en helt ny lagstiftning, som kräver stora investeringar innan den verksamhet som lagstiftningen förutsätter är helt uppbyggd. De brottsbekämpande myndigheterna bedömer att verksamheten successivt kommer att byggas upp under en period av fyra till fem år. För att kunna dra några säkra slutsatser om den nya lagens effektivitet och praktiska värde behöver därmed den nya lagens giltighetstid inte vara alltför kort. Lagen bör därför tidsbegränsas till att gälla i fem år.

20 Övriga frågor

20.1 Förhållandet till andra brottsbekämpande åtgärder

20.1.1 Bakgrund

Syftet med den nya lagen är att ge brottsbekämpande myndigheter möjlighet att kunna ingripa i cybermiljö. Det kommer framför allt att få betydelse för möjligheten att upptäcka brott. Frågan är då hur den nya lagstiftningen förhåller sig till andra brottsbekämpande åtgärder. Som tidigare har nämnts går det inte att förutse vad ett ingripande enligt den nya lagen kan resultera i, lika lite som vid ingripanden i den fysiska miljön.

I en del fall kan ett ingripande misslyckas t.ex. därför att det inte är möjligt för de brottsbekämpande myndigheterna att bereda sig tillgång till det aktuella informationssystemet eller därför att relevanta uppgifter har hunnit flyttas från det systemet till servrar eller andra informationssystem som inte är åtkomliga för svenska brottsbekämpande myndigheter. I fall där ett ingripande lyckas, i den meningen att det finns tydliga tecken på att det har förekommit brott eller brottslig verksamhet med hjälp av det eller de informationssystem som ingripandet har riktat sig mot, aktualiseras frågan hur den brottsbekämpande myndigheten ska gå vidare. Som framhållits tidigare syftar ingripandena inte till att samla material som kan användas för brottsutredning och lagföring. Ingripandena kommer däremot att kunna bekräfta eller avfärda de brottsbekämpande myndigheternas antagande att viss brottslig verksamhet pågår, som behöver förhindras. Det innebär att den kunskap som myndigheten får närmast kan jämföras med resultatet av andra polisiära spaningsmetoder.

Enligt utredningens mening finns det inte några sakliga skäl för att införa en annan reglering än den som gäller i dag för de brottsbekämpande myndigheternas hantering av den information som kan bli tillgänglig för dem genom ett ingripande i cybermiljö. Det hindrar emellertid inte att det kan uppstå särskilda problem i förhållande till dagens reglering. Det finns därför anledning att diskutera vissa sådana frågor, framför allt hur den nya lagstiftningen förhåller sig till regelverket om hemliga och preventiva tvångsmedel.

20.1.2 Inga författningsändringar krävs

Utredningens bedömning

Det behövs inga författningsändringar för att information från ingripanden i cybermiljö ska kunna användas i förundersökning eller för att berika underrättelseverksamhet.

Skälen för utredningens bedömning

När det saknas förutsättningar att utreda eventuellt brott

I många fall kan den information som blir tillgänglig genom ett ingripande i cybermiljö vara fragmentarisk. Det innebär att det inte finns tillräcklig substans beträffande en eller flera gärningar för att inleda förundersökning, trots att tröskeln för att göra det är låg. En annan tänkbar situation är att det vid ingripandet visserligen kan konstateras att det har förekommit brott, men att det inte finns några förutsättningar att utreda brottet. Det kan t.ex. bero på att det inte går att knyta informationssystemet till någon person, på det sätt som krävs i en förundersökning, och att det inte heller bedöms vara praktiskt möjligt att ta reda på vem som är skyldig till brottet (23 kap. 1 § andra stycket RB). Det kan även vara så att varken Sverige eller svenska intressen är berörda av brottet och att det därmed inte finns jurisdiktion för att utreda brottet här i landet. I sådana fall kan slutresultatet av ingripandet bli ett konstaterande att det inte finns någon rättslig grund för att inleda förundersökning.

När det finns underlag för att inleda förundersökning

Ett ingripande enligt den nya lagen kommer dock sannolikt i många fall att ge tillräckligt underlag för att inleda förundersökning, t.ex. om det har förekommit ett ransomwareangrepp riktad mot svenska juridiska eller fysiska personer eller om det finns anledning att anta att investeringsbedrägerier har drabbat svenska målsägande.

Det kan emellertid förutses att det ofta krävs viss tid innan den information som blivit tillgänglig genom ingripandet har hunnit analyseras närmare och det finns tillräcklig grund för att bedöma dels vilket brott det kan vara fråga om och om det kan knytas till någon person, dels om det finns svensk jurisdiktion för att utreda och lagföra brottet eller brotten. Det är emellertid inte något som skiljer sig från det som gäller för annan komplicerad eller svårutredd brottslighet.

I de fall där förundersökning inleds krävs det enligt utredningens mening inte några författningsändringar för att möjliggöra utredning av sådana brott som kan upptäckas genom ingripanden i cybermiljö. För sådana brott ska alltså de gällande bestämmelserna om förundersökning tillämpas.

När uppgifterna har betydelse för underrättelseverksamhet

Beroende på syftet med ett ingripande i cybermiljö kan resultatet av ingripandet bli att det kan berika underrättelseverksamheten. Det bör normalt vara fallet vid ingripanden för att upptäcka om ett informationssystem utnyttjas i brottslig verksamhet. I de fallen är syftet nämligen att avslöja om brottslig verksamhet pågår med hjälp av sådan teknisk utrustning som finns i Sverige. Det gäller även när ett ingripande görs i syfte att störa eller avbryta brottslig verksamhet i cybermiljö. Typiskt sett bör sådana ingripanden öka kunskapen om hur brotten begås, vilka målgrupper den brottsliga verksamheten riktas mot och vilka tekniska svagheter som har utnyttjats. I vissa fall kan de brottsbekämpande myndigheterna även få bättre kännedom om vilka personer eller grupperingar som kan ligga bakom brottsligheten. Om informationen från ingripandet inte är av intresse för svenska brottsbekämpande myndigheters underrättelseverksamhet kommer ärendet sannolikt att avslutas.

Underrättelseverksamheten är till största delen oreglerad (se avsnitt 13.1.1). Enligt utredningens mening krävs det därmed inte någon författningsändring för att eventuell information från ingripanden i cybermiljö ska få användas för att berika befintligt underrättelsematerial.

Särskilt om överskottsinformation

En särskild fråga är om det bör införas någon specifik reglering avseende den information som oavsiktligt kan bli tillgänglig genom ett ingripande i cybermiljö, dvs. en reglering av s.k. överskottsinformation. Särskilt mot bakgrund av att varje tillgång till digitala informationssystem potentiellt kan ge de brottsbekämpande myndigheterna tillgång till en stor mängd information om enskilda personer som saknar samband med det eller de brott eller den brottsliga verksamhet i cybermiljö som ingripandet avser är det befogat att diskutera den frågan. Det finns i dag en särskild reglering som rör överskottsinformation från hemliga och preventiva tvångsmedel. Den regleringen har nyligen gjorts mer enhetlig (prop. 2022/23:126 s. 170 f.). Däremot finns det inte någon reglering som avser överskottsinformation från andra åtgärder som brottsbekämpande myndigheter vidtar, exempelvis överskottsinformation från andra tvångsmedel än de hemliga eller preventiva tvångsmedlen.

Att överskottsinformation från hemliga och preventiva tvångsmedel regleras särskilt ska ses mot bakgrund av att syftet med sådana tvångsmedel är att i hemlighet samla in och analysera information, antingen för underrättelseverksamhet eller för att utreda och lagföra för brott. Det är då viktigt att tillgången till eventuell information om andra förhållanden än de som ligger till grund för användningen av tvångsmedlet, t.ex. om andra brott, regleras. Utan en sådan reglering har den som utsätts för tvångsmedlen inte tillräckliga möjligheter att reagera mot eventuella felaktigheter. Dessutom är regleringen av överskottsinformation från hemliga tvångsmedel något som Europadomstolen fäster vikt vid.

Som tidigare nämnts är utgångspunkten att ingripanden i cybermiljö normalt äger rum öppet. Syftet med ingripandena är inte att inhämta information. Sökningarna i informationssystemen görs enbart i syfte att genomföra själva ingripandet. Utom i de fall där för-

undersökning inleds, innebär det att det inte kommer att bevaras något material som härrör från sökningarna. Det innebär att de skäl som ligger bakom att överskottsinformation från hemliga och preventiva tvångsmedel regleras inte har samma relevans när det gäller information som härrör från ingripanden i cybermiljö. Sammantaget med kravet på att ingripanden i cybermiljö ska vara proportionerliga och inte får gå utöver vad som faktiskt behövs för att störa eller avbryta den brottsliga verksamheten eller för att förhindra eller avbryta brott innebär det att det saknas skäl att reglera eventuell överskottsinformation som ett ingripande i cybermiljö kan generera.

Internationellt samarbete

Eftersom brottslighet i cybermiljö i stor utsträckning är ett internationellt fenomen kan det förutses att många ingripanden i cybermiljö har internationella kopplingar. Det väcker frågan om det behövs några författningsändringar för att möjliggöra för den svenska polisen respektive Tullverket att kunna samarbeta effektivt med utländska brottsbekämpande myndigheter. Enligt utredningens mening är den lagstiftning som redan finns för internationellt polisiärt och tullrättsligt samarbete tillräcklig för att tillgodose behovet av att de svenska brottsbekämpande myndigheterna ska kunna lämna och ta emot information av betydelse för ingripanden i cybermiljö. Det behövs därmed inga författningsändringar.

20.1.3 Förhållandet till straffprocessuella tvångsmedel

Utredningens bedömning

Även om ingripanden enligt den nya lagen får göras mot brott och brottslig verksamhet både på underrättelsestadiet och på förundersökningsstadiet, behövs det inte några författningsändringar för att avgränsa tillämpningsområdet mot hemliga och preventiva tvångsmedel eller andra tvångsmedel.

Skälen för utredningens bedömning

En särskild fråga är hur den föreslagna regleringen förhåller sig till framför allt bestämmelserna om vissa hemliga och preventiva tvångsmedel men även genomsökning på distans.

Utredningen vill inledningsvis slå fast att syftet med den nya lagen inte är att ersätta något eller några av de befintliga tvångsmedlen. Däremot bör ingripanden enligt den nya lagen, inom ramen för underrättelseverksamhet eller förundersökning, förbättra förutsättningarna att störa och avbryta brottslig verksamhet och att förhindra eller avbryta brott. Om det inte är möjligt att förhindra eller avbryta brotten bör ingripanden enligt den nya lagen ses som ett steg på vägen till att kunna förbättra förutsättningarna för lagföring och fällande dom genom den kunskap som kan erhållas om bl.a. vilka personer eller företag som kan vara inblandade i brottsligheten. Om ingripandet leder till att ett brott avbryts, utesluter det inte att det i ett enskilt fall finns förutsättningar för lagföring och fällande dom.

Huvudskälet till att ingripanden enligt den nya lagen inte kan ersätta hemliga eller preventiva tvångsmedel är att det är fråga om kortvariga åtgärder. Syftena med straffprocessuella tvångsmedel respektive ingripanden enligt den nya lagen skiljer sig också åt på det sättet att syftet med ingripandena i cybermiljö – i motsats till det som gäller för hemliga och preventiva tvångsmedel – inte är att systematiskt och under längre tid samla in information (se bl.a. avsnitt 14.2 och 15.2).

Enbart det förhållandet att både hemlig dataavläsning och ingripanden i cybermiljö riktas mot informationssystem innebär inte att åtgärderna är utbytbara. Utgångspunkterna är helt olika, även om metoderna för att bereda sig tillgång till systemen är likartade. Kravet på att hemliga tvångsmedel och flertalet preventiva tvångsmedel ska kunna knytas till en person saknar motsvarighet i den nya lagen. Fokus i den nya lagstiftningen är i stället informationssystemen som sådana och deras funktion i den brottsliga verksamheten, för att kunna hejda den brottslighet som förekommer i dem. Det tillfälliga ingripandets huvudsyfte är att förhindra, störa eller avbryta brottsliga förehavanden. Då bör i många fall förutsättningarna för att använda hemliga eller preventiva tvångsmedel inte vara uppfyllda. Det kan emellertid även tänkas att initiativet till ingripandet i cybermiljö har sin grund i överskottsinformation från hemliga tvångsmedel, t.ex.

om en hemlig avlyssning avslöjar brottslig verksamhet som tidigare har varit okänd. Vidare är, som tidigare har nämnts, syftet med den nya lagstiftningen inte att samla in information i de syften som gäller för hemliga och preventiva tvångsmedel. Det finns därför ingen risk för att den nya lagen ska användas som en ersättning för sådana tvångsmedel.

När det gäller genomsökning på distans, som både får användas i förundersökning och i underrättelseverksamhet, kan konstateras att även det tvångsmedlet riktar sig mot digitala informationssystem. Det är ett straffprocessuellt tvångsmedel som enkelt uttryckt ersätter husrannsakan i digitala miljöer. Genomsökning på distans syftar till att söka efter handlingar som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen. Även i det fallet handlar det alltså om att samla in information i brottsutredande eller preventivt syfte. Inte heller när det gäller genomsökning på distans ser utredningen därför någon risk för att den nya lagstiftningen ska kunna användas som en ersättning för det tvångsmedlet.

Ett framgångsrikt ingripande i cybermiljö kan givetvis, som tidigare nämnts, leda till att personer blir misstänkta för brott och att, inom ramen för en förundersökning, tillstånd meddelas till användning av hemliga tvångsmedel. På motsvarande sätt kan ett sådant ingripande i vissa fall ge underlag för att i underrättelseverksamhet använda preventiva tvångsmedel. Varje tillstånd till ett hemligt eller preventivt tvångsmedel kräver emellertid att de särskilda rekvisiten för att tillämpa det är uppfyllda. Utredningen ser därmed inget behov av några författningsändringar för att avgränsa tillämpningsområdet för ingripanden i cybermiljö mot det som gäller för hemliga eller preventiva tvångsmedel eller genomsökning på distans.

20.1.4 Särskilt om barn

En särskild fråga som aktualiseras, mot bakgrund av att många barn och ungdomar i dag via kontakter i cybermiljö lockas att begå brott, är hur den nya lagstiftningen förhåller sig till barn under straffbarhetsåldern. Ingripanden enligt den nya lagen riktar sig mot informationssystem, och inte primärt mot personer. Normalt kommer den ingripande myndigheten inte att ha någon kännedom om vem som

använder informationssystemet i fråga och därmed inte heller hans eller hennes ålder. Det är i stället informationssystemet som sådant, uppgifterna i det och deras roll i brottsligheten som står i fokus. Det innebär att det i princip saknar betydelse för ingripandet vems uppgifter det är fråga om, vilken roll som personer som använder informationssystemet kan ha och deras ålder. Det är något som får betydelse först när frågan väcks om förundersökning ska inledas. I det avseendet skiljer sig inte ingripanden i cybermiljö från ingripanden i fysisk miljö.

Det bör samtidigt framhållas att barn i betydande utsträckning riskerar att falla offer för brott i cybermiljö. Om de brottsbekämpande myndigheterna får nya effektiva verktyg för att ingripa mot sådana brott kan det antas komma att gynna barn i större utsträckning än andra grupper.

20.2 Förhållandet till Försvarsmakten

20.2.1 Försvarsmakten ger stöd till polisen i den fysiska miljön

Även om de frågor som står i fokus för utredningen rör brottsbekämpning finns det anledning att kort beröra frågan om samarbete mellan Polismyndigheten, Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt vid viss verksamhet i cybermiljö. Antagonistisk verksamhet i cybermiljö är inte bara en fråga för brottsbekämpande myndigheter utan även för Försvarsmakten och Försvarets radioanstalt utifrån deras befintliga roller och mandat.

När det gäller ingripanden i fysisk miljö finns det reglerade samarbetsformer mellan polisen och Försvarsmakten i olika författningar, bl.a. lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning. Enligt 1 § den lagen får Polismyndigheten eller Säkerhetspolisen begära stöd under följande förutsättningar.

- Stödet behövs för att förhindra eller på annat sätt ingripa mot en handling som kan utgöra terroristbrott enligt 4 § terroristbrottslagen (2022:666) eller försök, förberedelse eller stämpling till, eller underlåtenhet att avslöja eller förhindra sådant brott.
- Ingripandet kräver resurser av särskilt slag som varken Polismyndigheten eller Säkerhetspolisen har tillgång till.

Dessutom ska regeringen ha lämnat sitt medgivande till stödet. Regeringens medgivande krävs dock inte i brådskande fall. Då ska begäran om stöd anmälas till regeringen omedelbart. Regeringen ska pröva om beslutet om stöd ska bestå eller undanröjas.

Enligt 2 § lagen om Försvarsmaktens stöd till polisen vid terrorismbekämpning ska Försvarsmakten ge stöd om den har resurser som är lämpliga och det inte medför synnerligt hinder i myndighetens ordinarie verksamhet. I 3 § föreskrivs att en enhet inom Försvarsmakten som ger stöd enligt lagen ska stå under befäl av en militär chef. När en stödinsats görs, ska enheten och dess chef stå under direkt ledning av den myndighet som har begärt stödet.

Enligt 2 § förordningen (2017:113) om Försvarsmaktens stöd till polisen med helikoptertransporter ska Försvarsmakten på begäran av polisen utföra helikoptertransporter som är av större vikt för genomförandet av polisiära insatser. Försvarsmakten får avslå begäran om det föreligger synnerliga skäl för annan användning av helikopterresursen. När stöd lämnas får enligt 3 § Försvarsmaktens personal inte användas i situationer där det finns risk för att den kan komma att bruka våld eller tvång mot enskilda.

20.2.2 Likartat stöd kan komma att behövas i cybermiljö

Någon reglering av samarbetsfrågor finns av naturliga skäl inte vid ingripanden i cybermiljö, eftersom polisens möjligheter att ingripa i den miljön är det som nu är föremål för utredning. Det kan emellertid enligt utredningens mening förutses att frågan om huruvida det behövs en likartad möjlighet till Försvarsmaktens och Försvarets radioanstalts stöd vid ingripanden i cybermiljö som i den fysiska miljön kan komma att aktualiseras. Det gäller särskilt om säkerhetsläget skulle försämras ytterligare. Det ligger utanför utredningens uppdrag att behandla de frågorna. Här kan dock konstateras att den reglering som utredningen föreslår inte lägger några hinder i vägen för samarbete mellan myndigheterna eller annat stöd som inte kräver lagreglering.

20.3 Skadeståndsfrågor

Utredningens bedömning

De nuvarande bestämmelserna om skadestånd ger goda möjligheter för en enskild vars informationssystem har varit föremål för ingripande i cybermiljö att begära skadestånd om regelverket har använts på ett felaktigt sätt. Det finns därför inte något behov av nya eller ändrade bestämmelser om rätt till skadestånd.

Skälen för utredningens bedömning

Allmänt om skadeståndsansvar

Enligt 3 kap. 1 § skadeståndslagen (1972:207) ska den som har en arbetstagare i sin tjänst ersätta bl.a. personskada eller sakskada som arbetstagaren vållar genom fel eller försummelse i tjänsten och ren förmögenhetsskada som arbetstagaren i tjänsten vållar genom brott. Vidare ska den som har arbetstagare i sin tjänst ersätta skada som arbetstagaren vållar genom fel eller försummelse i tjänsten på grund av att den allvarligt kränker någon annan genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära (kränkningsersättning).

För rätt till skadestånd på grund av ren förmögenhetsskada krävs det inte att skadevållaren har dömts till straff för gärningen (Bertil Bengtsson och Erland Strömbäck, Skadeståndslagen, En kommentar, JUNO version: 8C, 2025-10-29, kommentaren till 2 kap. 2 § och 3 kap. 1 §).

När det gäller rätt till kränkningsersättning vid vissa brott avses angrepp mot annans frid och den enskildes rätt att vara i fred och hålla sitt privatliv okänt för andra. Exempel som nämnts är ofredande, brytande av post- och telehemlighet, intrång i förvar och olovlig avlyssning i sådana fall där agerandet är ägnat att framkalla oro och ängslan hos den skyddade (Bertil Bengtsson och Erland Strömbäck, a.a., kommentaren till 2 kap. 3 § och 3 kap. 1 §). Ett annat exempel bör enligt utredningens mening kunna vara dataintrång.

Förmögenhetsbrott ger normalt ingen rätt till kränkningsersättning. Vid t.ex. skadegörelse som samtidigt innebär ett ofredande är kränkningsersättning inte uteslutet. Vad som är att anse som en all-

varlig kränkning får bedömas från fall till fall. Därvid bör samtliga relevanta omständigheter tillmätas betydelse. En allvarlig kränkning av den personliga integriteten förutsätter att angreppet riktar sig mot någon som åtminstone i viss mån värnar sin integritet (Ersättning för ideell skada, prop. 2000/01:68, s. 65 f.).

För skada som en arbetstagare vållar genom fel eller försummelse i tjänsten är han eller hon enligt 4 kap. 1 § skadeståndslagen ansvarig endast i den mån synnerliga skäl föreligger med hänsyn till handlingens beskaffenhet, arbetstagarens ställning, den skadelidandes intresse och övriga omständigheter. Avsikten med paragrafen är att den skadelidande ska kunna rikta sitt skadeståndskrav mot skadevållarens arbetsgivare och att arbetstagaren endast i undantagsfall ska bli skadeståndsansvarig (Bertil Bengtsson och Erland Strömbäck, a.a., kommentaren till 4 kap. 1 §).

Särskilt om statens skadeståndsansvar

Staten är enligt 3 kap. 2 § skadeståndslagen skyldig att ersätta bl.a. personskada, sakskada och ren förmögenhetsskada, som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten svarar. Staten är även skyldig att ersätta skada på grund av att någon annan allvarligt kränks genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära genom fel eller försummelse vid sådan myndighetsutövning.

En tjänsteman som uppsåtligen eller av oaktsamhet vid myndighetsutövning genom handling eller underlåtenhet åsidosätter vad som gäller för uppgiften kan dömas för tjänstefel om gärningen inte är ringa. Är gärningen straffbelagd enligt någon annan bestämmelse ska emellertid, enligt 20 kap. 1 § brottsbalken, den bestämmelsen tillämpas om den leder till samma eller stängare straff. Regleringen i 3 kap. 2 § skadeståndslagen innebär ett utvidgat skadeståndsansvar för staten genom att staten, om skadan vållas vid myndighetsutövning, svarar för ren förmögenhetsskada på samma sätt som vid person- eller sakskada. Myndighetsutövning kan sägas vara sådana beslut och åtgärder från myndighetens sida som är ett uttryck för myndighetens rätt att utöva makt över en enskild genom att den enskilde står i beroendeställning i förhållande till myndigheten. Det innebär att myndigheten bestämmer över den enskildes rättigheter

eller skyldigheter eller ingriper med faktiska åtgärder i den enskildes förhållanden, utan att han eller hon har rätt att motsätta sig den (Bertil Bengtsson och Erland Strömbäck, a.a., kommentaren till 3 kap. 2 §).

Staten ska vidare enligt 3 kap. 4 § skadeståndslagen ersätta bl.a. personskada, sakskada, ren förmögenhetsskada och skada på grund av att någon annan allvarligt kränks genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära genom fel eller försummelse vid sådan myndighetsutövning, om skadan uppkommit till följd av att den skadelidandes grundläggande fri- och rättigheter enligt 2 kap. RF eller enligt Europakonventionen har överträtts från statens sida, och annan ideell skada som uppkommit till följd av en sådan överträdelse.

Överträdelser av Europakonventionen

I Europakonventionen (inbegripet senare tillkomna tilläggsprotokoll till konventionen) anges en rad grundläggande fri- och rättigheter som konventionen omfattar. Vid överträdelse av rättigheter från en konventionsstats sida har enskilda klagorätt till Europadomstolen, som då kan meddela en för staten folkrättsligt bindande dom. Av särskild betydelse i sammanhanget är artikel 13, som föreskriver att den vars fri- och rättigheter enligt konventionen har kränkts ska ha rätt till ett effektivt rättsmedel inför en inhemsk domstol. Av intresse är vidare artikel 41, som ger Europadomstolen möjlighet att, om den nationella rätten endast till en del medger att gottgörelse lämnas för en överträdelse, kan tillerkänna den förfördelade skälig gottgörelse när så anses nödvändigt. Ett mål får inte tas upp av Europadomstolen innan alla nationella rättsmedel har uttömts. Det innebär att eventuella överträdelser av konventionen i största möjliga utsträckning ska rättas till på det nationella planet. Sverige är alltså skyldigt att säkerställa skyddet för de rättigheter som konventionen innebär, genom att tillhandahålla effektiva rättsmedel för enskilda som anser att någon rättighet har överträtts av det allmänna. Bestämmelserna i 3 kap. 4 § skadeståndslagen om skadestånd för överträdelser av konventionen är ett led i det systemet (Bertil Bengtsson och Erland Strömbäck, a.a., kommentaren till 3 kap. 4 §).

Regleringen i 3 kap. 4 § skadeståndslagen innebär att i den mån det är nödvändigt för att gottgöra en överträdelse – om andra rättsmedel inte är tillräckliga – ska skadestånd utges. Skadeståndsansvaret omfattar inte bara personskada, sakskada, allmän förmögenhetsskada och skada på grund av kränkning enligt 2 kap. 3 § skadeståndslagen utan också annan ideell skada. Ansvaret gäller oavsett om myndighetsutövning föreligger, vilket är en skillnad mot skadestånd enligt 3 kap. 2 § skadeståndslagen. I motsats till andra ansvarsregler enligt lagen anger inte lagtexten att vållande (uppsåt, vårdslöshet, fel eller försummelse) är en förutsättning för skadestånd (Bertil Bengtsson och Erland Strömbäck, a.a., kommentaren till 3 kap. 4 §).

Som utredningen har redovisat i avsnitt 19.3.2 kan Säkerhets- och integritetsskyddsnämnden anmäla till Justitiekanslern om den vid sin tillsyn uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person. Möjligheten att anmäla fel kommer att gälla även vid tillsyn över den nya lagen. Justitiekanslern prövar om anmälningar från nämnden om felaktigheter kan medföra skadeståndsansvar för staten. Justitiekanslern handlägger anspråk på ersättning med stöd av 2 kap. 1 § eller 3 kap. 1, 2 eller 4 § skadeståndslagen om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut (3 § 2 förordningen om handläggning av skadeståndsanspråk mot staten).

Slutsatser

Den enskilde har redan i dag, under de förutsättningar som anges i skadeståndslagen, rätt till ersättning för person- och sakskada, ren förmögenhetsskada och för kränkning som han eller hon drabbas av till följd av brottsbekämpande myndigheters ingripanden som inte beslutas eller verkställs på ett författningsenligt sätt. Det kommer även att gälla för ingripanden enligt den föreslagna nya lagen, om den införs. Därutöver har staten särskilt ansvar för överträdelser av de grundläggande fri- och rättigheter som tillförsäkras enskilda i Europakonventionen.

Det kan alltså konstateras att de befintliga bestämmelserna om skadestånd ger goda möjligheter för en enskild, vars informationssystem har varit föremål för ett ingripande i cybermiljö, att begära

skadestånd av staten om ingripandet inte har varit författningsenligt. Det finns därför inte något behov av mer långtgående bestämmelser om rätt till skadestånd än de som följer av de befintliga bestämmelserna.

20.4 Frågor om sekretess, tystnadsplikt och personuppgiftsbehandling

20.4.1 Sekretess

Utredningens bedömning

Känsliga uppgifter som kan avslöjas vid ingripanden i cybermiljö skyddas i tillräcklig utsträckning genom bestämmelserna i 18 och 35 kap. offentlighets- och sekretesslagen, men även av andra bestämmelser i den lagen. Det finns inget behov av nya sekretessbestämmelser eller några ändringar i de nuvarande sekretessbestämmelserna, varken till skydd för ingripanden i cybermiljö eller till skydd för enskilda.

Skälen för utredningens bedömning

Sekretessbestämmelser i brottsbekämpande verksamhet

För de verksamheter där den nya lagen kommer att tillämpas gäller framför allt sekretess enligt 18 och 35 kap. offentlighets- och sekretesslagen, som skyddar det allmännas respektive enskildas intressen i brottsbekämpande verksamhet.

Sekretess gäller hos Säkerhetspolisen, Polismyndigheten, Tullverket, Åklagarmyndigheten och Ekobrottsmyndigheten även enligt t.ex. 15 kap. offentlighets- och sekretesslagen till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer. Sådana sekretessbestämmelser som gäller generellt, exempelvis bestämmelser i 21 kap., är också tillämpliga. I 7 kap. 3 § offentlighets- och sekretesslagen regleras vad som gäller när flera sekretessbestämmelser samtidigt är tillämpliga på en uppgift hos en myndighet.

Sekretessbestämmelser till skydd för brottsbekämpning

I 18 kap. offentlighets- och sekretesslagen finns det en rad sekretessbestämmelser till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet.

Sekretess till skydd för förundersökningar och liknande utredningar

Enligt 18 kap. 1 § första stycket gäller sekretess för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Enligt andra stycket gäller sekretess, under motsvarande förutsättningar, för uppgift som hänför sig till verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde (punkten 1) eller annan verksamhet än sådan som avses i 1 eller i första stycket som syftar till att förebygga, upptäcka, utreda eller beivra brott och som bedrivs av bl.a. en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller Tullverket (punkten 2).

Med förundersökning avses i paragrafen förundersökning enligt RB. Av 2 kap. 10 § TF följer att handlingar som framställts i en förundersökning och som alltjämt finns hos myndigheten inte ska anses utgöra allmänna handlingar förrän förundersökningen har avslutats eller, om handlingarna ingår i förundersökningsprotokollet, det har färdigställts.

En s.k. förutredning är att betrakta som ett led i tillämpningen av bestämmelserna i 23 kap. 1 § RB. Med förutredning brukar avses sådana enstaka åtgärder som en förundersökningsledare ibland behöver vidta för att få tillräckligt underlag för beslut om huruvida förundersökning ska inledas eller inte. Förutredning är ett i princip oreglerat förstadium till förundersökning och regleras alltså inte direkt av 23 kap. RB (Eva Lenberg m.fl., Offentlighets- och sekretesslagen, JUNO Version: 32, 2025-12-05, Norstedts Juridik, kommentaren till 18 kap. 1 § och 35 kap. 8 a §).

Tvångsmedel i brottmål avser framför allt de straffprocessuella tvångsmedel som regleras i 24–28 kap. RB och i lagen om hemlig dataavläsning. Tvångsmedel i annan verksamhet för att förebygga brott anses vara sådana tvångsmedel som avses i preventivlagen, inhämtningslagen, lagen om särskild kontroll av vissa utlänningar och lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

Med annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott avses Åklagarmyndighetens, Ekobrottsmyndighetens, Polismyndighetens, Säkerhetspolisens eller Tullverkets brottsförebyggande och brottsbeivrande verksamhet i allmänhet, utan anknytning till något konkret fall (Eva Lenberg m.fl., a.a., kommentaren till 18 kap. 1 §). Regleringen anses vara tillämplig även vid utredning av brott i utredningar enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare (prop. 2000/01:109 s. 17).

Paragrafen har ett rakt skaderekvisit, dvs. utgångspunkten är att uppgifterna är offentliga. Sekretessen gäller endast om följden av att uppgifterna lämnas ut kan antas bli att syftet med beslutade eller förutsedda åtgärder motverkas eller att den framtida verksamheten skadas. Här åsyftas åtgärder och verksamhet för att på olika stadier bekämpa brottsligheten. Med åtgärder förstås främst beslut och ingripanden som hänför sig till ett särskilt ärende. En uppgift, vars röjande t.ex. kan försvåra en pågående brottsutredning, kan alltså hållas hemlig.

Sekretess till skydd för underrättelseverksamhet m.m.

I 18 kap. 2 § offentlighets- och sekretesslagen regleras sekretess för uppgifter som hänför sig till verksamhet hos bl.a. Polismyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen och Tullverket för att förebygga, förhindra eller upptäcka brottslig verksamhet.

Enligt 18 kap. 2 § första stycket gäller sekretess för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 1 § 1 lagen polisens behandling av personuppgifter inom brottsdatalagens område, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Sekretessen gäller med ett omvänt skaderekvisit. Utgångspunkten är att alltså att uppgifterna omfattas av sekretess.

Föremålet för sekretessen är personuppgiftsbehandling hos Polismyndigheten om uppgifterna behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet, hos Ekobrottsmyndigheten om uppgifterna behandlas i syfte att utreda brott och det inte är fråga om åklagarverksamhet, och hos Säkerhetspolisen i frågor som inte rör nationell säkerhet, om uppgifterna behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Enligt 18 kap. 2 § andra stycket gäller sekretess, under motsvarande förutsättningar, för uppgift som hänför sig till sådan verksamhet som bl.a. avses i 2 kap. 1 § 1 lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område (punkten 1). Föremålet för sekretessen är personuppgiftsbehandling hos Tullverket, om den är nödvändig för att myndigheten ska kunna förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd, eller fullgöra förpliktelser som följer av internationella åtaganden.

Vidare gäller sekretess under motsvarande förutsättningar för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 1 § 1 lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Det innebär att Säkerhetspolisen får behandla personuppgifter om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar a) brott mot Sveriges säkerhet, b) terrorbrott, eller c) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv.

Sekretess i verksamhet hos den som biträder bl.a. polisen

Enligt 18 kap. 3 § offentlighets- och sekretesslagen gäller sekretessen enligt 1 och 2 §§ i annan verksamhet än sådan som avses där hos en myndighet för att biträda bl.a. en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller Tullverket med att förebygga, uppdaga, utreda eller beivra brott.

Bestämmelsen innebär att, om skaderekvisitet är uppfyllt, sekretess kan upprätthållas för t.ex. en myndighets utredning till grund för åtalsanmälan, obduktionsutlåtande och utlåtande av vetenskapligt laboratorium. Sekretessen gäller redan innan uppgifterna har

kommit åklagare eller polis till del (Eva Lenberg m.fl., a.a., kommentaren till 18 kap. 3 §).

Sekretess till skydd för vissa metoder

Enligt 18 kap. 9 § offentlighets- och sekretesslagen gäller sekretess för uppgift som lämnar, eller kan bidra till upplysning om, chiffer, kod eller liknande metod, om det kan antas att syftet med metoden motverkas om uppgiften röjs och metoden har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts (punkten 1) eller att göra det möjligt att kontrollera om data i elektronisk form har förvanskats (punkten 2).

Sekretessen är begränsad till uppgifter som avser att slå vakt om sekretessen i allmän verksamhet. Chiffret ska alltså ha till syfte att underlätta befordran eller användning av uppgifter som omfattas av sekretess. För det ändamålet används bl.a. kryptering. Den metoden används t.ex. för att befordra meddelanden genom tele- eller datakommunikation. Informationen förvanskas genom krypteringen till oigenkännlighet och kan på så sätt befordras utan att den röjs för obehöriga. Det är krypteringsnyckeln eller koden som sekretesskyddas. Bestämmelsen är tillämplig även på förvaring av krypterat material. Det kan naturligtvis förekomma att chifferspråk används för meddelanden som inte innehåller uppgifter som omfattas av sekretess eller för vilka sekretess efter en tid inte längre gäller. Även sådana meddelanden i klartext kan hållas hemliga så att chiffret inte kan forceras. Bestämmelsen tar främst sikte på intresset att förebygga eller beivra brott. Sekretessen gäller endast om ett röjande av uppgiften kan antas motverka syftet med chiffret, dvs. att slå vakt om sekretessen i allmän verksamhet.

Sekretess kan även gälla för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att göra det möjligt att kontrollera om data i elektronisk form har förvanskats. Användningen av elektroniska signaturer på myndighetsområdet förutsätter att hemliga nycklar och anknytande uppgifter för bl.a. elektronisk signering och autentisering kan skyddas mot insyn. Lagen (2000:832) om kvalificerade elektroniska signaturer syftar till att underlätta användningen av elektroniska signaturer. Genom sekretessbestämmelsen är det möjligt att sekretessbelägga

t.ex. hemliga nycklar som används för att verifiera om en handling härrör från angiven undertecknare eller för att skydda vissa datamängder mot manipulation. Sekretessen gäller med ett rakt skaderekvisit. Utgångspunkten är alltså att uppgifterna är offentliga.

Sekretess till skydd för internationellt polissamarbete

Enligt 18 kap. 17 a § offentlighets- och sekretesslagen gäller sekretess hos brottsbekämpande myndigheter för uppgift som lämnats av ett utländskt organ inom ramen för internationellt polisiärt samarbete i syfte att förebygga, uppdaga, utreda eller beivra brott, om det kan antas att en förutsättning för att uppgiften lämnades var att den inte skulle röjas.

Med internationellt polisiärt samarbete avses alla former av polisiärt samarbete, både sådant som tar sikte på enskilda fall och sådant som rör de brottsbekämpande myndigheternas arbete i stort. Utanför begreppet faller utredning enligt bestämmelserna om förundersökning i brottmål eller en angelägenhet som angår tvångsmedel. Det utländska organ som lämnar uppgifterna kan t.ex. vara en utländsk brottsbekämpande myndighet eller en mellanfolklig organisation som Interpol.

Sekretessen är inte begränsad till uppgifter med ett visst innehåll eller av viss art eller karaktär. Uppgiften måste dock ha lämnats i brottsbekämpande syfte. Det kan röra sig om t.ex. en förfrågan eller en upplysning som skickas ut till samtliga länder inom Interpol. Det kan också röra sig om en förfrågan från ett samarbetsland om huruvida en viss person förekommer i svenska register eller om några åtgärder vidtagits i fråga om en viss person eller ett visst föremål.

Sekretessen gäller endast om det kan antas att en förutsättning för att uppgifterna lämnades var att de inte skulle röjas. Mot bakgrund av att det inom det internationella polisiära samarbetet ofta förutsätts att känsliga uppgifter kan skyddas i den anmodade staten innebär skaderekvisitet att det råder en presumtion för sekretess. Sekretessen gäller bara hos brottsbekämpande myndigheter, dvs. i första hand Polismyndigheten, Säkerhetspolisen och Tullverket. Även uppgifter som finns hos Åklagarmyndigheten och i åklagarverksamheten hos Ekobrottsmyndigheten kan skyddas av bestämmelsen om uppgiften har lämnats i ett brottsbekämpande syfte vid

internationellt polisiärt samarbete (Eva Lenberg m.fl., a.a., kommentaren till 18 kap. 17 a §).

Sekretessbestämmelser till skydd för enskildas personliga och ekonomiska förhållanden

I 35 kap. offentlighets- och sekretesslagen regleras sekretess för uppgifter om enskildas personliga eller ekonomiska förhållanden i brottsbekämpande verksamhet.

Enligt 35 kap. 1 § första stycket offentlighets- och sekretesslagen gäller sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer hos bl.a. Polismyndigheten, Säkerhetspolisen, Tullverket eller åklagarmyndighet och uppgiften har anknytning till brottsutredningar eller annan brottsbekämpande verksamhet. Vidare gäller sekretess för uppgifter som förekommer i olika register som förs av brottsbekämpande myndigheter. Regleringen korresponderar i princip med sekretessbestämmelserna i 18 kap. 1–3 §§ offentlighets- och sekretesslagen till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Till skillnad från regleringen i 18 kap. 1 § gäller sekretessen enligt 35 kap. 1 § offentlighets- och sekretesslagen med ett omvänt skaderekvisit, vilket innebär en presumtion för sekretess.

I 35 kap. 2, 6 och 7 §§ görs vissa undantag från regleringen i 35 kap. 1 § första stycket offentlighets- och sekretesslagen.

Enligt 35 kap. 8 a § offentlighets- och sekretesslagen hindrar sekretessen enligt 1 § inte att en enskild som har varit anmäld eller misstänkt för brott tar del av en uppgift, om han eller hon har beaktansvärda skäl för sin begäran att få ta del av uppgiften, och det inte bedöms vara av synnerlig vikt för den som uppgiften rör eller någon närstående att uppgiften inte lämnas ut. Det gäller när uppgiften förekommer i en förundersökning som har lagts ned eller avslutats med ett beslut om att åtal inte ska väckas (punkten 1), eller en annan brottsutredning om brottet som har utförts enligt bestämmelserna i 23 kap. RB och som har avslutats på något annat sätt än genom beslut att väcka åtal, eller att utfärda strafföreläggande eller föreläggande av ordningsbot (punkten 2). Bestämmelsen gäller även för den

som varit misstänkt i en s.k. förutredning (Eva Lenberg m.fl., a.a., kommentaren till 35 kap. 8 a §).

Slutsatser

Det är viktigt att känsliga uppgifter skyddas av sekretess som gäller både till skydd för det allmännas verksamhet och till skydd för enskilda. Vid ett ingripande i cybermiljö kan känsliga uppgifter avslöjas både under det förberedande stadiet och när ingripandet genomförs. Enligt utredningens mening skyddas känsliga uppgifter som kommer fram under ett ingripande i tillräcklig utsträckning av de nuvarande bestämmelserna i 18 och 35 kap. offentlighets- och sekretesslagen, men även av övriga sekretessbestämmelser i den lagen. Det finns därför inte behov av några nya sekretessbestämmelser eller några ändringar i de befintliga sekretessbestämmelserna.

20.4.2 Tystnadsplikt

Utredningens förslag

Operatörers tystnadsplikt enligt 9 kap. 32 § LEK ska även omfatta en begäran om medverkan enligt den nya lagen.

Skälen för utredningens förslag

I avsnitt 18.4 har utredningen föreslagit att operatörer som har anmälningsplikt enligt 2 kap. 1 § LEK ska vara skyldiga att medverka vid ingripanden enligt den nya lagen. I 9 kap. 32 § LEK föreskrivs i dag tystnadsplikt för uppgifter om vissa åtgärder som kan vidtas av brottsbekämpande myndigheter. Det gäller bl.a. uppgifter om hemliga tvångsmedel. För att ingripanden i cybermiljö inte ska avslöjas i förtid är det viktigt att information om en begäran om medverkan enligt den nya lagen inte blir offentlig. Den tystnadsplikt som gäller enligt 9 kap. 32 § LEK bör därför omfatta även en sådan begäran.

20.4.3 Lagstiftningen om personuppgiftsbehandling

Utredningens bedömning

Det krävs inga ändringar i lagstiftningen om personuppgiftsbehandling.

Skälen för utredningens bedömning

Personuppgiftsbehandlingen i brottsbekämpande verksamhet regleras på ett övergripande sätt i brottsdatalagen och brottsdataförordningen (2018:1202). De författningarna kompletteras av sektorsvisa lagar och förordningar. Av intresse här är lagen om polisens behandling av personuppgifter inom brottsdatalagens område med tillhörande förordning, lagen om Tullverkets behandling av personuppgifter inom brottsdatalagens område med tillhörande förordning och lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område med tillhörande förordning. Behandling av personuppgifter som rör nationell säkerhet regleras i lagen om Säkerhetspolisens behandling av personuppgifter med tillhörande förordning.

De befintliga författningarna om personuppgiftsbehandling på området reglerar i stort sett all personuppgiftsbehandling i brottsbekämpande verksamhet, från underrättelseverksamhet till lagföring. I den utsträckning som det kommer att krävas behandling av personuppgifter vid ingripanden enligt den nya lagen eller som annars kan aktualiseras med anledning av den nya lagstiftningen, täcks behandlingen enligt utredningens mening av den befintliga lagstiftningen om personuppgiftsbehandling. Det finns inte heller i övrigt något behov av ändring av lagstiftningen om personuppgiftsbehandling med anledning av utredningens förslag.

20.5 Behovet av följdändringar

Utredningens förslag

En bestämmelse införs i tullbefogenhetslagen som hänvisar till Tullverkets rätt att ingripa enligt den nya lagen.

Utredningens bedömning

I övrigt krävs det inga följdändringar i nuvarande lagstiftning.

Skälen för utredningens förslag och bedömning

En hänvisningsbestämmelse i tullbefogenhetslagen

Genom tullbefogenhetslagen har Tullverkets befogenheter i brottsbekämpande verksamhet samlats i en lag. När det därefter har införts nya befogenheter för myndigheten genom en separat lag har det införts en hänvisning som anger det i tullbefogenhetslagen (se 7 kap. 3 a §). En motsvarande hänvisningsbestämmelse bör enligt utredningens mening införas som påminner om de befogenheter som Tullverket ges i den nya lagen. Bestämmelsen kan lämpligen placeras i 7 kap. tullbefogenhetslagen. Rubriken på det kapitlet bör då justeras något.

Det behövs inga andra följdändringar

Den nya lagen har få beröringspunkter med annan lagstiftning som gäller i dag. Utredningen har därför inte kunnat finna att det behövs följdändringar i någon annan lagstiftning.

21 Överväganden om integritetsintrånget

21.1 Bakgrund

I övervägandena om de förslag som har lämnats har utredningen löpande kommenterat förhållandet till RF och Europakonventionen. Utredningen har också i kapitel 19 föreslagit olika åtgärder som ska motverka de integritetsrisker som den nya lagstiftningen kan leda till. I avsnitt 20.1 har utredningen vidare redovisat hur den nya regleringen förhåller sig till befintliga regler om brottsutredning och lagföring. För att tydliggöra hur enskildas rätt till privatliv och integritet balanseras mot de brottsbekämpande myndigheternas behov av ytterligare verktyg för att ingripa mot brottslighet i cybermiljö, redovisas här en mer samlad bild.

21.2 Balansen mellan brottsbekämpning och enskildas rättssäkerhet

21.2.1 Förslagen leder normalt till integritetsintrång

Utredningens bedömning

Det är oundvikligt att ingripanden i cybermiljön, på samma sätt som ingripanden i den fysiska miljön, normalt leder till visst integritetsintrång. Intrånget varierar dock beroende på vad ingripandet riktas mot, vilken åtgärd som vidtas och hur ingripandet genomförs.

Skälen för utredningens bedömning

Visst intrång är oundvikligt

Redan det förhållandet att ett första steg i ett ingripande i cybermiljö normalt är att den brottsbekämpande myndigheten bereder sig tillgång till ett informationssystem innebär ett integritetsintrång. Även om den nya lagen riktar sig mot informationssystemen som sådana, inte mot de personer som äger eller använder systemen, kommer ingripandena att påverka dem. Det gäller oavsett om myndigheten inte har lyckats vidta någon åtgärd i systemet efter det att den har berett sig tillträde till det eller om det har vidtagits omfattande åtgärder.

Av de åtgärder som de brottsbekämpande myndigheterna föreslås få använda är radering normalt mer ingripande än andra. Mot den bakgrunden föreslås en mer kvalificerad beslutsfattare och högre krav för att radering ska få beslutas. Även blockering kan i ett enskilt fall leda till större intrång än andra åtgärder. Det har utredningen tagit hänsyn till när det gäller behovet av underrättelse. För alla ingripanden enligt lagen ställs det krav på att de ska vara proportionerliga. Vidare föreslår utredningen att beslutsfattaren alltid ska överväga om ett beslut om ingripande ska förenas med villkor. Det innebär att ingripandena alltid ska anpassas så att integritetsintrånget för enskilda begränsas.

Intrånget varierar

Enligt utredningens mening kommer integritetsintrånget att variera både beroende på vilken typ av informationssystem, eller del av system, eller vilka uppgifter som ingripandet riktar sig mot och på vilken åtgärd som vidtas.

När det gäller informationssystem kan konstateras att de möjligheter att agera anonymt som skapas genom det digitala samhället har lockat till sig kriminalitet. Brott och brottslighet i cybermiljö sträcker sig från rekrytering av kontraktsmördare, marknadsplatser för försäljning av narkotika och systematiska bedrägerier till enskilda ungdomar som trakasserar kamrater. Det är därför svårt att generellt ange vilket integritetsintrång som den nya lagen kan medföra.

Eftersom den nya lagen kommer att kräva teknisk expertis, vilket är en trång sektor för de brottsbekämpande myndigheterna, förutser

utredningen att ingripandena framför allt kommer att riktas mot följande fyra kategorier av brottslighet i cybermiljö

1. brottslighet som ingår i organiserad och systematisk brottslighet, ofta bedriven av kriminella nätverk i Sverige, eller utomlands, t.ex. organiserade bedrägeribrott och utpressningsangrepp,
2. brottslighet som riktas mot Sveriges säkerhet, kritisk infrastruktur och annan samhällsviktig verksamhet eller utgör terroristbrottslighet,
3. brottslighet där personer medverkar till eller beställer tjänster i form av sexuella övergrepp mot barn, och
4. brottslighet där personer köper illegala varor som narkotika och vapen på Darknet och andra digitala plattformar.

I de nu aktuella fallen kommer integritetsintrånget alltså främst att påverka personer eller nätverk som antingen planerar eller deltar aktivt i den aktuella brottsligheten. Utredningen anser att de personerna eller nätverken normalt räknar med att kunna utsättas för polisiära ingripanden. Detsamma gäller främmande makt. En annan sak är att regelverket för ingripanden ska hålla hög juridisk standard och vara rättssäkert.

De åtgärder som vidtas inom ramen för ett ingripande kan också differentieras genom hur ingripande de kan vara. Den åtgärd som kan förväntas leda till minst intrång är ingripanden för att kartlägga om ett informationssystem utnyttjas i brottslig verksamhet. I den andra änden av skalan finns radering. Även radering kan dock leda till varierande intrång, beroende bl.a. på mängden uppgifter som raderas. Övriga ingripanden kan, beroende på hur de genomförs, leda till varierande intrång.

Ett ingripande som förutsätter att myndigheten bereder sig tillträde till en viss plats får typiskt sett anses leda till större intrång än ingripanden som genomförs på annat sätt.

21.2.2 Åtgärder som motverkar intrånget

Utredningens bedömning

Det integritetsintrång som ingripanden i cybermiljö kan leda till vägs upp av olika förslag som minimerar risken för felaktiga och alltför omfattande ingripanden.

Skälen för utredningens bedömning

Rättssäkerhetsgarantier är viktigt

För att motverka det integritetsintrång som kan uppstå vid ingripanden i cybermiljö har utredningen föreslagit en rad bestämmelser, för att minimera risken för felaktiga eller alltför omfattande ingripanden. Även om integritetsintrång vid ingripanden i cybermiljö främst kommer att påverka personer som är inblandade i brottslig verksamhet är rättssäkerhetsgarantier viktiga.

Tydliga krav på beslut och genomförande

Utformningen av lagstiftningen och de krav som ställs på beslut om ingripanden i cybermiljö har stor betydelse för bedömningen av integritetsintrånget. Utredningen vill särskilt framhålla att en differentiering har gjorts mellan de olika formerna av ingripanden på det sättet att det i flera avseenden ställs högre krav på den åtgärd som normalt kan leda till störst integritetsintrång, nämligen radering. I det fallet ställs det högre krav för att beslut om radering ska få fattas. För radering krävs att raderingen är av synnerlig vikt för ändamålet. För andra åtgärder är det tillräckligt att åtgärden är av särskild vikt. Vidare ska åklagare besluta om radering, medan beslut om andra åtgärder får fattas av särskilda befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket. Det ställs också särskilda krav på kompetens på sådana befattningshavare, som i vissa brådskande situationer får fatta interimistiska beslut om radering. De besluten ska i så fall prövas i efterhand av åklagare.

För att säkerställa att ingripanden inte görs i miljöer som normalt skyddas mot ingripanden på grund av att det där förekommer upp-

gifter som har anförtrotts vissa yrkeskategorier, bl.a. journalister, advokater och präster, föreskrivs förbud mot att ingripanden riktas mot vissa informationssystem och vissa uppgifter.

Ett generellt krav som ställs på alla beslut om ingripanden och som gäller även för verkställigheten är som nämnts att ingripandena ska vara proportionerliga. Det är ett uttryckligt lagkrav.

Något som kommer att bidra till att ingripanden bara görs när det finns sakliga skäl för det är kraven på skriftliga beslut och en generell skyldighet att dokumentera beslut och åtgärder enligt den nya lagen. Det bidrar till eftertanke hos den som föreslår att ett ingripande ska göras och till att beslutsfattaren noga tvingas tänka igenom vad ingripandet ska omfatta och hur det ska genomföras. Detsamma gäller kravet på att beslutsfattaren alltid ska överväga om ett ingripande bör förenas med villkor.

Vidare ska ett beslut om ingripande, t.ex. en blockering, upphävas när det inte längre finns skäl för åtgärden. Det garanterar att beslut inte gäller längre än vad som är sakligt motiverat.

Efterföljande kontroll

Utredningen föreslår i avsnitt 19.3 att det ska utövas särskild tillsyn över tillämpningen av den nya lagen och att den uppgiften ska läggas på Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd.

Den särskilda tillsynen ska vara en rättslig tillsyn. Nämnden kan genom inspektioner och uttalanden bl.a. verka för en mer enhetlig rättstillämpning och kan även lyfta fram eventuella oklarheter eller svagheter i lagstiftningen.

Den extraordinära tillsyn som utövas av JO och Justitiekanslern tillkommer utöver den särskilda tillsynen.

Tidsbegränsad lagstiftning

Ett ytterligare sätt att skapa balans mellan behovet av nya effektiva verktyg för att bekämpa allvarlig brottslighet och att värna den personliga integriteten är att inte göra den nya lagstiftningen permanent. I avsnitt 19.4 föreslår utredningen att lagen ska tidsbegränsas att gälla i fem år. Även om det inte påverkar integritetsintrånget

under den tid som lagen gäller, är det ett sätt att, efter en tids tillämpning, tvinga fram en omprövning av lagstiftningen. Det behövs för att klargöra både om lagstiftningen har uppfyllt de förväntningar som ställs på den och om den har en fått en adekvat utformning. Då finns det även möjlighet att väga resultaten av den nya regleringen mot det intrång i den personliga integriteten som regleringen kan ha lett till.

21.2.3 Utredningens samlade bedömning av intrånget i den personliga integriteten

Utredningens bedömning

I relation till de vinster för brottsbekämpningen som kan förväntas med de nya verktyg som föreslås, anser utredningen att intrånget i den personliga integriteten är godtagbart.

Skälen för utredningens bedömning

Vid en samlad bedömning anser utredningen att det intrång i den personliga integriteten som ett ingripande i cybermiljö enligt den nya lagen kan medföra balanseras väl av de rättssäkerhetsgarantier som har byggts in i lagen.

Utredningen har övervägt olika andra alternativ att utforma regleringen. Det gäller bl.a. frågan om vissa beslut bör vara överklagbara eller kunna prövas i efterhand på annat sätt (avsnitt 16.2.4). En annan sådan fråga är hur långt de ingripande myndigheternas underrättelseskyldighet bör sträcka sig (avsnitt 19.1.1 och 19.1.2). Även frågan om det bör införas ett uttryckligt förbud för den ingripande myndigheten att vid ett ingripande hämta in uppgifter från ett informationssystem har övervägts. En sådan reglering skulle dock enligt utredningens mening kunna skapa sådana tekniska hinder mot vissa ingripanden att den nya lagstiftningen riskerar att bli verkningslös.

I avvägningen mellan vinsten av att brottsbekämpande myndigheter kan ingripa effektivt i cybermiljö och det intrång som kan följa av tillämpningen av lagen får enligt utredningen mening intrånget i den personliga integriteten anses vara godtagbart. Bedömningen ska

ses mot bakgrund av den allvarliga brottslighet som pågår i cybermiljö och det sätt på vilket kriminella utnyttjar informationssystem, samtidigt som de brottsbekämpande myndigheterna i dag saknar effektiva verktyg för att bekämpa den brottsligheten. Nya möjligheter att bekämpa brott och brottslighet i cybermiljö innebär också en viktig förbättring för brottsoffer.

21.3 Utredningens förslag i förhållande till grundläggande fri- och rättigheter

Utredningens bedömning

Förslagen är förenliga med kraven i RF, Europakonventionen, EU:s rättighetsstadga och barnkonventionen.

Skälen för utredningens bedömning

Regeringsformen, Europakonventionen och EU:s rättighetsstadga

Som framgår av avsnitt 3.2–3.4 måste den nya lagstiftningen, för att motsvara kraven i RF och Europakonventionen, uppfylla både de krav som ställs på lagstiftning som innebär inskränkningar i privatlivet och de krav som ställs på ett förfarande som säkerställer en rättvis rättegång.

Utgångspunkten i RF och Europakonventionen är att grundläggande fri- och rättigheter inte får inskränkas på annat sätt än genom lag. Det kravet uppfylls genom förslaget till en ny lag om polisiära ingripanden i cybermiljö. Vidare krävs att inskränkningarna är godtagbara i ett demokratiskt samhälle och nödvändiga med hänsyn till bl.a. förebyggande och skydd mot brott. Behovet av ingripanden är väl underbyggt och regleringen går inte utöver vad som är godtagbart mot bakgrund av den allvarliga brottsutvecklingen. Det bör även framhållas att ingripandena i första hand riktar sig mot informationssystem, inte mot enskilda personer.

Enligt RF får inskränkningarna inte heller utgöra ett hot mot den fria åsiktsbildningen. Utredningen bedömer att det inte utgör någon reell risk, så som förslagen har utformats, bl.a. eftersom det i lagen införs både ett förbud mot att rikta ingripanden mot journalistisk verksamhet och en uttrycklig proportionalitetsregel.

Ett generellt krav som ställs på bestämmelser som innebär inskränkningar i grundläggande fri- och rättigheter är att lagstiftningen ska vara tydlig och förutsebar. Det är då viktigt att bestämmelserna om vilka åtgärder som får vidtas och förutsättningarna för att använda dem är tydliga. Vidare krävs att lagens tillämpningsområde är tillräckligt anpassat. Utredningen anser att kraven på en tydlig och förutsebar lagstiftning är uppfyllda.

Skyddet enligt EU:s rättighetsstadga ligger i linje med skyddet enligt Europakonventionen. Det som nyss har sagts om förenligheten med Europakonventionen gäller därmed även EU:s rättighetsstadga.

Barnkonventionen

Utredningen kan inte finna att den nya lagstiftningen i något avseende skulle stå i strid med barnkonventionen (se avsnitt 3.6). Tvärtom bör den nya lagstiftningen bidra till att minska risken för att barn utsätts för brott i cybermiljö.

22 Ikraftträdande och övergångsbestämmelser

22.1 Ikraftträdande

Utredningens förslag

Den nya regleringen ska träda i kraft den 1 juli 2027. Lagen och förordningen tidsbegränsas och ska gälla till och med den 30 juni 2032.

Skälen för utredningens förslag

Hoten från brottslighet i cybermiljö har ökat under en längre tid. Det är därför angeläget att de brottsbekämpande myndigheterna ges betydligt bättre förutsättningar att kunna ingripa i den miljön. Även om utredningen har förståelse för att det kommer att ta viss tid innan de brottsbekämpande myndigheterna har byggt upp full kapacitet på området bör den föreslagna lagstiftningen träda i kraft så snart som möjligt. Utredningen bedömer att det bör vara möjligt att låta lagstiftningen träda i kraft den 1 juli 2027. Av de skäl som anförts i avsnitt 19.4 bör lagen och förordningen tidsbegränsas att gälla till och med utgången av juni 2032.

22.2 Övergångsbestämmelser

Utredningens bedömning

Det behövs inga övergångsbestämmelser.

Skälen för utredningens bedömning

Utgångspunkten när det gäller processrättslig lagstiftning är att nya bestämmelser ska tillämpas genast efter ikraftträdandet. Det innebär att de tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. Den ordningen är tillämplig när det gäller den föreslagna nya lagen om polisiära ingripanden i cybermiljö. Utredningen anser därför att det inte finns något behov av särskilda övergångsbestämmelser för den nya regleringen och inte heller för övriga ändringar som föreslås.

23 Konsekvenser

23.1 Allmänt om konsekvenserna

Utredningens förslag innebär att en ny lag, lagen om polisiära ingripanden i cybermiljö, med tillhörande förordning införs. Genom lagen ges Polismyndigheten, Säkerhetspolisen och Tullverket rätt att ingripa mot brott och brottslig verksamhet i cybermiljö. Att det är fråga om en ny reglering, som dessutom kommer att kräva uppbyggnad av en helt ny verksamhet, som förutsätter särskild teknisk och juridisk kapacitet, gör det svårare än normalt att uppskatta såväl de kostnader som övriga konsekvenser som förslaget kan leda till.

23.2 Kraven på en konsekvensutredning

Det framgår av kommittéförordningen (1998:1474) och 6–11 §§ förordningen (2024:183) om konsekvensutredningar att utredningen ska redovisa konsekvenserna av de förslag som lämnas i betänkandet. Utredningen ska bedöma och redovisa förslagens ekonomiska och andra konsekvenser, bl.a. konsekvenserna för det brottsbekämpande arbetet och den personliga integriteten.

Av direktiven för utredningen framgår att särskild vikt ska läggas vid effekterna för rättsväsendets myndigheter. Utredningen ska beskriva och, när det är möjligt, kvantifiera de samhällsekonomiska effekterna av de förslag som läggs. De offentligfinansiella effekterna av utredningens förslag ska beräknas. Om förslagen innebär finansiella kostnader ska förslag till finansiering lämnas enligt 15 § kommittéförordningen.

Utredningen ska även bedöma och redovisa hur förslagen förhåller sig till RF, mediegrundlagarna, EU-rätten inklusive EU:s rättighetsstadga samt Sveriges internationella åtaganden om mänskliga

rättigheter inklusive barnkonventionen. De frågorna har behandlats i avsnitt 21.3. Utredningen ska även redovisa vilka konsekvenser som de förslag som lämnas har ur ett barnrättsperspektiv samt ur ett jämställdhetsperspektiv.

Av direktiven framgår också att utredningen ska analysera den samlade regleringens konsekvenser för den personliga integriteten. Frågor om konsekvenserna för den personliga integriteten behandlas i kapitel 21. Det som framgått i nämnda kapitel kommer inte att upprepas här.

23.3 Ekonomiska konsekvenser för myndigheterna

23.3.1 Allmänt om förslagets ekonomiska påverkan

Ingripanden i cybermiljö grundas enligt förslaget på en helt ny lagstiftning, som kräver stora investeringar i teknik, utbildning och personal, innan den verksamhet som lagstiftningen förutsätter är helt uppbyggd. Myndigheterna behöver bygga upp nya funktioner för att hantera de nya möjligheterna att ingripa. Samtliga myndigheter avser att införa en ny central funktion.

De investeringar i nya it-system och andra verktyg som krävs ligger till största delen utanför den normala teknikutvecklingen i de berörda myndigheterna. Den nya lagstiftningen kommer därför att medföra kostnader, utöver de kostnader för teknikutveckling som myndigheterna har begärt medel för till den nuvarande it-verksamheten.

Som redan nämnts är det är mycket svårt att beräkna kostnaderna. Det beror på att en ny ingripandeverksamhet som är helt teknikberoende successivt måste byggas upp, samtidigt som tekniken fortsätter att utvecklas i snabb takt. Utredningen kan därför bara göra en mycket grov uppskattning, baserad bl.a. på erfarenheterna från införandet av hemlig dataavläsning. Den reformen hade stora likheter med förslaget till en ny lag i fråga om behovet teknikuppbyggnad. Utredningens kostnadsberäkningar bygger på det preliminära underlag som de brottsbekämpande myndigheterna har presenterat.

Polismyndigheten, Säkerhetspolisen och Tullverket bedömer att verksamheten successivt kommer att byggas upp, under en period av 4–5 år. Vissa kostnader för teknikutveckling, anställning av personal,

anskaffning och anpassning av lokaler m.m. kommer emellertid att belasta anslagen redan från början. Vid beräkningen av kostnaderna har myndigheterna beaktat att den nya lagstiftningen kan innebära effektivitetsvinster i form av minskad brottslighet, effektivare brottsutredningar och det förhållandet att ingripanden kan göras digitalt i stället för fysiskt. Även de synergieffekter som kan uppstå genom samarbete mellan de berörda myndigheterna kring vissa tekniska eller praktiska lösningar har beaktats. Det är mot bakgrund av det sagda tydligt att kostnaderna för reformen inte ryms inom myndigheternas nuvarande anslag.

Myndigheterna har beräknat att antalet ingripanden totalt i vart fall inte kommer att understiga 500 ärenden per år när verksamheten är uppbyggd.

Eftersom det rör sig om grova uppskattningar och utvecklingen kan komma att leda till fler ingripanden än som angetts, samtidigt som andra faktorer – som inte nu kan förutses – kan komma att påverka kostnaderna, kan det visa sig att kostnaderna kan bli högre än som anges i det följande.

Kostnaderna är beräknade per helår. Om ikraftträdandet beslutas till en annan tidpunkt än ett årsskifte, vilket utredningen föreslår, förändras följaktligen kostnaden för det första verksamhetsåret.

Det ska slutligen noteras att de ekonomiska konsekvenserna som anges inte kommer att vara aktuella om lagen om polisiära ingripanden i cybermiljö inte permanentas efter de fem åren som förslaget omfattar.

De samhällsekonomiska vinsterna av förslagen är ännu svårare att beräkna än kostnaderna. Utredningen avstår därför från att försöka kvantifiera dem. De består emellertid bl.a. i att

- tryggheten i samhället ökar,
- risken för cyberangrepp mot vitala delar av staten och mot samhällsviktiga strukturer minskar,
- risken för cyberangrepp mot företag och enskilda minskar,
- möjligheterna att skaffa olagliga droger online begränsas, och
- vinsterna för kriminella nätverk minskar.

23.3.2 Polismyndigheten

Utredningens förslag

Anslaget till Polismyndigheten ska höjas med 120 miljoner kronor det första verksamhetsåret, 180 miljoner kronor det andra året, 220 miljoner kronor det tredje året, 260 miljoner kronor det fjärde året och 300 miljoner kronor det femte året.

Skälen för utredningens förslag

Polismyndigheten har för budgetåret 2026 ett totalt anslag om 48,376 miljarder kronor.

Polismyndigheten har bedömt att ingripanden enligt den nya lagen på sikt kommer att beslutas mer eller mindre dagligen. Ingripandena förväntas vara av olika karaktär, från mycket komplexa ingripanden i cybermiljö som kräver lång förberedelsetid och mycket kvalificerad teknisk expertis, till enklare ärenden som t.ex. enbart består av radering av enstaka uppgifter.

De beräknade framtida kostnaderna omfattar personal (särskilt teknisk personal som är både svårrekryterad och extra kostnadskrävande), lokaler (nya lokaler krävs) och it-verksamhet (uppbyggnad av teknisk kapacitet, utbildning, driftskostnader, avskrivningar på teknisk utrustning, licenser alternativt abonnemang och löpande teknikutveckling). Vidare tillkommer kostnader för utökat samarbete med andra myndigheter och med näringslivet samt internationellt samarbete.

Polismyndighetens anslag bör enligt utredningens mening höjas med 120 miljoner kronor det första året (varav 20 miljoner kronor för personal), 180 miljoner kronor det andra året (varav 30 miljoner kronor för personal), 220 miljoner kronor det tredje året (varav 40 miljoner kronor för personal), 260 miljoner kronor det fjärde året (varav 50 miljoner kronor för personal) och slutligen, 300 miljoner kronor det femte året (varav 60 miljoner kronor för personal). Polismyndigheten bedöms också ha behov av en utökad låneram.

Polismyndigheten har framhållit att myndigheten i ett första skede kommer att fokusera på en nationell tillämpning av lagen, för att därefter successivt låta lagen och det arbete som följer med den steg för steg etableras regionalt. Om lagen permanentas efter de föreslagna

fem åren behövs det därför en ny genomlysning av myndighetens kostnader för ingripanden enligt lagen.

23.3.3 Säkerhetspolisen

Utredningens förslag

Anslaget till Säkerhetspolisen ska höjas med 20 miljoner kronor det första verksamhetsåret, 40 miljoner kronor det andra året, 60 miljoner kronor det tredje året och vardera 90 miljoner kronor det fjärde respektive femte året.

Skälen för utredningens förslag

Säkerhetspolisen har för budgetåret 2026 ett totalt anslag om 3,048 miljarder kronor.

Säkerhetspolisen har bedömt att ingripanden enligt den nya lagen kan förekomma åtminstone varje vecka. Ingripandena förväntas vara av olika karaktär, från mycket komplexa ingripanden i cybermiljö som kräver lång förberedelsetid och mycket kvalificerad teknisk expertis till vissa enklare ärenden.

De beräknade framtida kostnaderna omfattar personal (särskilt teknisk personal som är både svårrekryterad och extra kostnadskrävande), lokaler (huvudsakligen anpassning av befintliga) och it-verksamhet (uppbyggnad av teknisk kapacitet, utbildning, driftskostnader, avskrivningar på teknisk utrustning, licenser alternativt abonnemang och löpande teknikutveckling). Vidare tillkommer kostnader för utökat samarbete med andra myndigheter och med näringslivet samt internationellt samarbete.

Säkerhetspolisens anslag bör enligt utredningens mening höjas med 20 miljoner kronor det första verksamhetsåret (varav 10 miljoner kronor för personal), 40 miljoner kronor det andra året (varav 20 miljoner kronor för personal), 60 miljoner kronor det tredje året (varav 30 miljoner kronor för personal), 90 miljoner kronor (varav 42 miljoner kronor för personal) både det fjärde året och det femte året. Säkerhetspolisen kan även behöva en utökad låneram.

Även Säkerhetspolisen har påpekat att om lagen permanentas behövs det en ny genomlysning av myndighetens kostnader för ingripanden enligt lagen.

23.3.4 Tullverket

Utredningens förslag

Anslaget till Tullverket ska höjas med 15 miljoner kronor det första verksamhetsåret, 20 miljoner kronor det andra året, 30 miljoner kronor det tredje året, 40 miljoner kronor det fjärde året och 50 miljoner kronor det femte året.

Skälen för utredningens förslag

Tullverket har för budgetåret 2026 ett totalt anslag om 3,44 miljarder kronor.

Tullverket har bedömt att ingripanden enligt den nya lagen kan förekomma åtminstone varje vecka. Ingripandena förväntas vara av olika karaktär, från mycket komplexa ingripanden i cybermiljö som kräver lång förberedelsetid och mycket kvalificerad teknisk expertis till vissa enklare ärenden.

De beräknade framtida kostnaderna omfattar personal (särskilt teknisk personal som är både svårrekryterad och extra kostnadskrävande), lokaler (både nya lokaler och viss anpassning av befintliga) och it-verksamhet (uppbyggnad av teknisk kapacitet, utbildning, driftskostnader, avskrivningar på teknisk utrustning, licenser alternativt abonnemang och löpande teknikutveckling). Vidare tillkommer kostnader för utökat samarbete med andra myndigheter och med näringslivet samt internationellt samarbete.

Tullverkets anslag bör höjas med 15 miljoner kronor det första verksamhetsåret (varav 5 miljoner kronor för personal), 20 miljoner kronor det andra året (varav 7 miljoner kronor för personal), 30 miljoner kronor det tredje året (varav 10 miljoner kronor för personal), 40 miljoner kronor det fjärde året (varav 12 miljoner kronor för personal) och 50 miljoner kronor det femte året (varav 14 miljoner kronor för personal). Tullverkets låneram kan också behöva höjas.

Även Tullverket har framhållit att om lagen permanentas behövs det en ny genomlysning av myndighetens kostnader för ingripanden enligt lagen.

23.3.5 Åklagarväsendet

Utredningens förslag

Anslaget till Åklagarmyndigheten ska höjas med 1,2 miljoner kronor det första verksamhetsåret och därefter med 1,2 miljoner kronor vart och ett av de följande fyra åren.

Skälen för utredningens förslag

Åklagarmyndigheten har för budgetåret 2026 ett totalt anslag på 2,891 miljarder kronor. Ekobrottsmyndigheten har för budgetåret 2026 ett totalt anslag på 1,218 miljarder kronor.

Åklagares roll enligt den nya lagen är begränsad. Den inskränker sig till att fatta beslut i de fall där radering aktualiseras och att pröva om interimistiska beslut om radering som har fattats av befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket har rättslig grund.

Åklagarmyndigheten har beräknat en extra kostnad om 1 miljon kronor för uppbyggnad av it-kapacitet. Eventuella it-kostnader bör enligt utredningens bedömning rymmas inom befintligt anslag. Det kommer däremot att krävas viss personalresurs som inte ryms inom det befintliga anslaget. Åklagarmyndighetens anslag bör därför höjas med 1,2 miljoner kronor årligen under fem år. Beroende på hur stor ärendetillströmning som kan bli fallet kan ytterligare personalkostnader tillkomma. Om lagen permanentas behövs en ny genomlysning av myndighetens kostnader.

Ekobrottsmyndigheten förväntas få ett begränsat antal ärenden, vilket inte kommer att innebära några merkostnader för myndigheten som inte ryms inom befintligt anslag.

23.3.6 Myndigheten för säkerhet och integritetsskydd

Utredningens förslag

Anslaget till Myndigheten för säkerhet och integritetsskydd ska höjas med 5,9 miljoner kronor det första verksamhetsåret och med 4 miljoner kronor per år under andra–femte åren.

Skälen för utredningens förslag

Myndigheten för säkerhet och integritetsskydd har för budgetåret 2026 ett totalt anslag på 48 miljoner kronor.

Utredningen har föreslagit att särskild tillsyn över den nya lagen ska utövas av Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd. Det är en liten myndighet och tillsynsuppgiften är helt ny. Den skiljer sig också från de tillsynsuppgifter som nämnden har i dag. Därför krävs det resurstillskott i form av fler föredragande, teknisk expertis, ombyggnad av lokalerna och vissa kringkostnader. Av samma skäl som angetts för anslagen till de brottsbekämpande myndigheterna bör anslaget till Myndigheten för säkerhet och integritetsskydd ge möjlighet till anställning av personal redan det första året, eftersom det är viktigt att tillsynen kan fungera från det att den nya lagen träder i kraft.

Anslaget för Myndigheten för säkerhet och integritetsskydd bör därför höjas med 5,9 miljoner kronor det första året (varav 4 miljoner kronor avser personal) och därefter med 4 miljoner kronor vardera det andra till femte året (för personal). Om lagen permanentas behövs det en ny genomlysning av myndighetens kostnader för tillsyn över lagen.

23.4 Konsekvenserna för brottsligheten

Utredningens bedömning

Utredningen bedömer att lagen får en avhållande effekt när det gäller brott och brottslig verksamhet i cybermiljö. Lagen kommer också att bidra till att, om fler brott som begås i cybermiljö upptäcks, de brotten i större utsträckning än i dag antingen kommer att kunna förhindras eller avbrytas eller, om så inte är fallet, att det finns bättre förutsättningar att utreda dem.

Skälen för utredningens bedömning

Den nya lagen ger brottsbekämpande myndigheter nya verktyg för att bekämpa brott och brottslighet i cybermiljö. Regleringen förväntas leda till en betydligt effektivare brottsbekämpning än i dag. De verktyg som kriminella använder för att undgå upptäckt och lagföring kan nämligen genom förslagen mötas med effektiva motåtgärder. Mot bakgrund av att särskilt personer som ägnar sig åt organiserad brottslighet snabbt anpassar sig till de rättsliga möjligheter som myndigheterna har, kan vissa brottsfenomen förväntas minska avsevärt. Den ökade upptäcktsrisken kommer att verka avhållande. Viss brottslighet kommer sannolikt att riktas mot måltavlor i andra länder än Sverige. De ekonomiska vinster som de kriminella nätverken får genom brott i cybermiljö kan också förväntas minska. Nya möjligheter att ingripa mot informationssystem som används av företrädare för organiserad brottslighet, som utnyttjar avancerade metoder för att förbli anonyma, ökar förutsättningarna att spåra de som anstiftar allvarliga brott i Sverige. Därigenom bör viss organiserad brottslighet kunna hållas tillbaka.

Genom tillämpningen av lagen kommer svenska myndigheters kunskaper både om hur brott i cybermiljö begås och vilka som kan ligga bakom organiserad brottslighet i den miljön att öka. Även om det främsta syftet med lagen är att förhindra brott och brottslighet i cybermiljö, kommer brottslighet av det slaget inte att försvinna. Det kan däremot förutses att, om fler brott som begås i cybermiljö upptäcks, förutsättningarna för att utreda brotten, i den mån de ligger inom svensk jurisdiktion, kommer att förbättras.

En stor vinst ligger också i att om den svenska lagstiftningen erbjuder goda möjligheter att ingripa mot brott i cybermiljö minskar incitamenten för främmande makt och för kriminella att utnyttja svensk infrastruktur för sådana ändamål. Det minskar risken att Sverige blir en fristad för cyberbrottslighet.

En modern svensk lagstiftning mot cyberbrott kommer även att ge svenska myndigheter möjlighet att utveckla det internationella samarbetet, vilket kan ge Sverige fördelar när det gäller annat samarbete mot bl.a. organiserad brottslighet.

I förhållande till allmänheten kommer den nya lagstiftningen att leda till ökat förtroende. Om förutsättningarna att bekämpa brott i cybermiljö förbättras, kan benägenheten att anmäla sådana brott förväntas öka. Inte minst möjligheten att radera övergreppsmaterial och att förhindra att exempelvis stulna personuppgifter och kontokortsuppgifter säljs vidare kommer att bidra till ökad trygghet i samhället.

23.5 Konsekvenserna för det brottsförebyggande arbetet

Utredningens bedömning

Den nya lagen förväntas ge positiva effekter för det brottsförebyggande arbetet.

Skälen för utredningens bedömning

När det gäller det brottsförebyggande arbetet förväntas den nya regleringen också ge positiva effekter. Den främsta förebyggande effekten nås genom att den nya lagstiftningen tydligt markerar att svenska myndigheter har möjlighet att ingripa mot cyberbrott som riktar sig mot Sverige och svenska intressen, vilket kommer att förebygga sådana cyberbrott som riktas mot det land som har de sämsta möjligheterna att agera mot sådana brott.

Ingripanden mot olika former av crime as a service innebär att färre personer kommer att lockas in i kriminalitet genom de ”annonser” om brottsuppdrag som i dag attraherar unga, ofta ostraffade

personer. Det är särskilt viktigt att kunna förebygga nyrekryteringen till kriminella nätverk.

Enklare möjligheter att blockera och kunna stänga ner marknadsplatser där bl.a. narkotika, vapen och sexuella övergrepp erbjuds till försäljning kommer att leda till att många brott kan förebyggas. På samma sätt kommer förbättrade möjligheter att kunna stänga platser på digitala plattformar som förespråkar terrorism och bidrar till radikalisering att leda till att terroristbrott förebyggs.

De ökade kunskaper som de brottsbekämpande myndigheterna får genom ingripanden i cybermiljö kommer att ge positiva effekter även för bekämpning av brott generellt, vilket är av stor betydelse eftersom de allra flesta brott innehåller digitala inslag numera.

23.6 Övriga samhällskonsekvenser

23.6.1 Konsekvenserna för barn

Utredningens bedömning

Förslagen får inte några särskilda konsekvenser för barn.

Skälen för utredningens bedömning

Utredningens förslag om en lag om polisiära ingripanden i cybermiljö, leder inte till några särskilda konsekvenser för barn. Det bör anmärkas att unga i särskilt stor utsträckning använder de möjligheter som cybermiljön skapar och att de därför, i större utsträckning än vuxna, kan riskera att drabbas av brott i den miljön. Som tidigare nämnts är det positivt för barn som utsätts för brott i cybermiljö att myndigheterna får bättre möjligheter att ingripa mot sådana brott. Det bör minska risken för att barn utsätts för sexuella övergrepp i cybermiljö. Det bör även minska risken för att barn dras in i kriminalitet.

Det bör framhållas att unga personer, som visserligen har uppnått straffbarhetsåldern, kan riskera att påverkas mer negativt av att bli utsatta för ingripanden enligt den nya lagen i jämförelse med vuxna. Det samlade integritetsintrånget har som tidigare nämnts behandlats i kapitel 21.

23.6.2 Konsekvenserna för jämställdheten

Utredningens bedömning

Förslagen får inte några konsekvenser för jämställdheten.

Skälen för utredningens bedömning

Utredningens förslag är utformade så att de inte innebär olika konsekvenser för män och kvinnor respektive pojkar och flickor. Förslagen bedöms inte heller på annat sätt påverka jämställdheten. Det går dock att sluta sig till att det – mot bakgrund av hur brottsligheten ser ut – främst är män och pojkar som kommer att beröras av utredningens förslag.

23.6.3 Konsekvenserna i övrigt

Utredningens bedömning

Den nya lagen kommer att få positiva effekter för små företags arbetsförutsättningar. Förslagen får inte några andra sådana konsekvenser som framgår av 15 § kommittéförordningen och som inte har behandlats i detta kapitel.

Skälen för utredningens bedömning

Utredningen bedömer att den nya lagen kommer att få positiva effekter för små företags arbetsförutsättningar, eftersom sådana företag inte i samma utsträckning som i dag riskerar att utsättas för olika typer av cyberangrepp.

Utredningen bedömer inte att förslagen i övrigt får några sådana konsekvenser som anges i 15 § kommittéförordningen som ska redovisas i betänkandet, dvs. konsekvenser för sysselsättning och offentlig service i olika delar av landet, konkurrensförmåga eller villkor i övrigt i förhållande till större företag eller för möjligheterna att nå de integrationspolitiska målen.

24 Författningskommentar

24.1 Förslaget till lag (2027:000) om polisiära ingripanden i cybermiljö

Lagens innehåll

1 §

Paragrafen innehåller en övergripande beskrivning av lagens innehåll. Den har behandlats i avsnitt 13.1.1.

Lagen, som är ny, ger Polismyndigheten, Säkerhetspolisen och Tullverket befogenhet att ingripa mot brott och brottslig verksamhet som helt eller delvis begås i cybermiljö. Ingripanden kan göras både på underrättelsestadiet, för att störa, förhindra eller avbryta brottslig verksamhet, och på utredningsstadiet, för att förhindra eller avbryta brott. Lagen är vidare tillämplig för att förhindra framtida brott, utan att det pågår någon brottsutredning eller särskilt inriktad underrättelseverksamhet. Ändamålen med ingripandena regleras i 3–5 §§.

Med brott avses ett konkret brott. Det krävs dock inte att gärningens alla detaljer är kända, exempelvis exakt när och var brottet ska begås eller har begåtts och vem brottet riktar eller har riktat sig mot. Inte heller behöver det finnas någon känd gärningsman.

Med brottslig verksamhet avses en inte närmare preciserad verksamhet som innefattar ett eller flera kriminaliserade handlanden. Det innebär att handlingen inte behöver uppfylla rekvisiten för ett visst konkret brott, utan endast kan vara tecken på någon identifierbar form av brottslighet. Det kan vara fråga om flera brott som har samband med varandra t.ex. genom brottstyp, handlingssätt eller gärningsmannaskap eller enskilda brott som begås som ett led i en mer eller mindre organiserad kriminell verksamhet. Systematiska investerings- eller romansbedrägerier kan vara exempel på det förstnämn-

da och grov narkotikabrottslighet som bedrivs av kriminella nätverk på det sistnämnda. Den brottsliga verksamheten kan också bestå i erbjudande om kriminella tjänster, t.ex. sexualbrott som begås ”på beställning”, eller erbjudanden om försäljning av droger, dopningsmedel eller vapen.

Ingripandena kan i princip avse vilken typ av brott eller brottslighet som helst; det enda kravet är att det är fråga om brott som begås i cybermiljö. Tillämpningsområdet begränsas emellertid i 6 § till brott av viss svårhetsgrad.

Begreppet cybermiljö används för att avgränsa tillämpningsområdet mot ingripanden i den fysiska miljön. I cybermiljön ingår den virtuella miljön som består av digitalt skapade och tekniskt sammanlänkade utrymmen där information utbyts, kommunikation sker och händelser initieras – utan att de nödvändigtvis är bundna till ett visst geografiskt territorium eller en fysisk plats. Med cybermiljö avses alltså en övergripande miljö eller domän där digital information skapas, bearbetas, kommuniceras och lagras. Begreppet omfattar alla former av verksamhet och kommunikation som äger rum på bl.a. internet, inkluderande digitala miljöer i form av webben, sociala medier och andra digitala plattformar, koder, dataflöden, protokoll, algoritmer och digitala interaktioner. Även teknisk infrastruktur som datorer, nätverk, servrar, fiberoptik, hårdvara och andra digitala system som utgör grunden för den digitala miljön ingår i begreppet.

Lagens tillämpningsområde

2 §

Paragrafen, som avgränsar lagens tillämpningsområde, har behandlats i avsnitt 13.2–13.6.

Lagen är endast tillämplig på brott, som begås eller kommer att begås i cybermiljö, eller på brottslig verksamhet som innefattar sådana brott. Vad som avses med cybermiljö framgår av kommentaren till 1 §. En grundläggande förutsättning för att lagen ska vara tillämplig är att ett inslag i brotten eller brottsligheten är användning av elektroniska informationssystem i cybermiljö. Det kan innebära antingen att användning av internet är en direkt förutsättning för att brottet ska kunna begås, t.ex. ett överbelastningsangrepp, eller att användningen av internet enbart är ett medel för att begå ett brott

som lika gärna kan begås i fysisk miljö, exempelvis bedrägeri, utpressning eller sexuella övergrepp på barn.

Regleringen innebär emellertid inte att lagen är generellt tillämplig på brott eller brottslig verksamhet enbart för att t.ex. en modern mobiltelefon utnyttjas i planeringen av brottet eller som ett sätt att hålla kontakt mellan inblandade personer medan gärningen begås i den fysiska miljön. Utanför tillämpningsområdet faller exempelvis telefonsamtal som förs i syfte att planera, förbereda eller utföra brott i den fysiska miljön. I de fallen används informationssystemet inte som ett medel för att begå brotten utan enbart som ett sätt att kommunicera mellan två eller flera personer. Då kan i stället traditionella tvångsmedel användas. Vid sådana kontakter i en chattfunktion som utgör led i brottet, t.ex. rekrytering av någon som ska genomföra brottet, kan lagen däremot vara tillämplig.

Det är tillräckligt att något rekvisit i en straffbestämmelse har koppling till cybermiljö för att brottet ska uppfylla kravet på att det begås eller kommer att begås i cybermiljö. Det kan t.ex. vara att vilseledandet i ett bedrägeri äger rum genom kontakter på internet eller att initierandet av smuggling av narkotika görs genom beställningar på en hemsida på Darknet. Ett annat exempel är att bomber tillverkas efter instruktioner som hämtas från internet.

I begreppet informationssystem ingår hårdvara, mjukvara, databaser och nätverkskomponenter som samverkar för att samla in, lagra, bearbeta eller överföra uppgifter utan kontinuerlig manuell styrning. Ett informationssystem innefattar all slags befintlig och framtida teknisk utrustning som kan användas för att kommunicera elektroniskt, t.ex. datorer, mobiltelefoner, läsplattor, interaktiva högtalare, servrar, smarta klockor och annan liknande utrustning. Utrustning som är sammankopplad med sådan utrustning, fysiskt eller på annat sätt, t.ex. sladdar, tangentbord, usb-minnen, datormus och andra elektroniska tillbehör omfattas också av begreppet. Begreppet ska däremot inte tolkas så vitt att ett helt nätverk, som en dator är kopplad till genom en sladd, och all utrustning som är ansluten till nätverket, oavsett storleken på nätverket, ingår i det informationssystem som ingripandet får riktas mot. Avgränsningen av vad ingripandet kan rikta sig mot ska göras utifrån vad som framstår som rimligt med hänsyn till det informationssystem som berörs.

Med informationssystem avses i lagen även ett användarkonto, eller en på motsvarande sätt avgränsad del av, en kommunikations-

tjänst, lagringstjänst eller annan liknande tjänst. Gemensamt för sådana tjänster är att det är möjligt att få tillgång till uppgifter i dem från olika elektroniska kommunikationsutrustningar när användaren anger t.ex. inloggningsuppgifter. Det gäller oberoende av var uppgifterna är lagrade. Även internetbaserade tjänster vilkas primära syfte inte är kommunikation eller lagring, men som innefattar möjlighet till något av det, ryms i begreppet informationssystem (jfr prop. 2019/20:64 s. 103, 105 och 211).

Som framgått av kommentaren till 1 § är lagen tillämplig på såväl brottslig verksamhet som brott, innefattande osjälvständiga brottsformer. Däremot är lagen inte avsedd att användas för att utreda eller lagföra brott. Genom att den brottsliga verksamheten ska innefatta brott görs en koppling till 6 § som innehåller krav på att brotten ska vara av viss svårhetsgrad.

För att ett ingripande enligt lagen ska kunna riktas mot ett visst informationssystem krävs det tillräcklig information för att kunna identifiera det. Sådan information kan ha kommit till de brottsbekämpande myndigheternas kännedom på olika sätt, t.ex. genom en brottsanmälan från en målsägande. Ett annat exempel kan vara att det vid en husrannsakan, en genomsökning på distans eller genom ett hemligt tvångsmedel har framkommit att ett visst informationssystem används för brott eller brottslig verksamhet.

Med att brott begås avses någon pågående form av brottslighet som är på planeringsstadiet eller senare. Att även brott ”kommer att begås” omfattas hör samman med att ett viktigt syfte med ingripanden enligt lagen är att förhindra framtida brott, t.ex. terroristbrott och spridning av barnpornografi.

I tre punkter anges vilken anknytning som ska finnas till Sverige för att lagen ska vara tillämplig. Regleringen ska ses mot bakgrund bl.a. av att syftet med lagen är att kunna ingripa redan innan ett konkret brott har begåtts och att det då ännu inte finns någon sådan anknytning till brottet som förutsätts i 2 kap. brottsbalken. Anknytningsfaktorerna är alternativa. Det innebär att det är tillräckligt att en av dem är uppfylld för att lagen ska bli tillämplig. De två första punkterna i paragrafen motsvarar i huvudsak regleringen i 2 kap. 1 § brottsbalken och återspeglar territorialitetsprincipen, som är en grundprincip för jurisdiktion. Den tredje punkten har sin bakgrund i att brott i cybermiljö skiljer sig från brott i fysisk miljö, eftersom

det i de förstnämnda fallen inte alltid behöver finnas någon fysisk person som ligger bakom de enskilda brotten.

Enligt *punkten 1* är lagen tillämplig på brott som begås eller kommer att begås av någon som fysiskt befinner sig i Sverige. Brott i cybermiljö förutsätter normalt att en person, med hjälp av ett informationssystem, initierar ett händelseförlopp t.ex. ett ransomwareangrepp. Den som har påbörjat brottet behöver inte vara samma person som senare ställer krav på en lösensumma eller som kontaktar brottsoffret i ett investerings- eller romansbedrägeri. Lagen är alltså tillämplig om gärningsmannen eller gärningsmännen, eller annan medverkande, befinner sig i Sverige.

I *punkten 2* görs lagen även tillämplig på brott som riktas mot någon eller något som befinner sig i Sverige. Det saknar då betydelse var den person befinner sig som utför den aktivitet i cybermiljö som resulterar i eller kan komma att resultera i ett brott i Sverige. Det är i stället effekten av brottet eller brotten eller det tänkta målet för brotten som gör lagen tillämplig. Det kan röra sig om brott som är avsedda att orsaka ekonomisk eller annan skada eller fara som kan uppstå i Sverige. Genom att ange att brottet ska riktas mot någon omfattas dels brott riktade mot fysiska personer i Sverige (oavsett om brottet riktar sig mot en obekant krets av sådana personer eller en viss person), dels brott riktade mot juridiska personer i Sverige i form av företag, myndigheter, kommuner eller andra motsvarande organ.

Ett brott anses normalt sett vara riktat mot den som är att bedöma som målsägande, dvs. den mot vilken brott har begåtts eller som har blivit förnärmad eller lidit skada av brottet (20 kap. 8 § fjärde stycket RB). För att lagen ska vara tillämplig är det alltså tillräckligt att syftet med brottet är att nå måltavlor i Sverige. När det gäller t.ex. bedrägeri genom annonser på internet kan sådana omständigheter som att annonseringen är på svenska eller på annat sätt tydligt riktar sig mot en svensk publik vara tillräckligt för att punkten ska vara tillämplig.

Ingripanden kan även avse brott som riktar sig mot den svenska staten. Det gäller t.ex. brott som i sin helhet begås utomlands men där brottet riktar sig mot ett intresse som den svenska staten uppfattas som bärare av. Det kan röra sig om brott mot rikets säkerhet, allmän verksamhet eller annat av rättsordningen särskilt skyddat svenskt intresse. Dit hör brott mot svenska statens yttre eller inre

säkerhet eller mot offentliga myndigheter. Regleringen omfattar även t.ex. smuggling och brott mot svensk valutareglering.

Det tänkta målet för brottet kan även vara ett informationssystem som finns i Sverige, utan att det finns en koppling till något av de nyss nämnda subjekten. Genom formuleringen ”eller något” omfattas således även brott som riktar sig mot enbart föremål i Sverige. Det innebär att lagen även är tillämplig på exempelvis dataintrång som uteslutande har som mål att skaffa sig tillgång till föremål i Sverige som är uppkopplade mot internet. Typiskt sett kan det vara fråga om att elektronisk utrustning i Sverige används som ett led i anonymiseringsnätverk, för att dölja gärningsmannens identitet. Det kan även röra sig om utpressnings- eller bedrägeriangrepp som slumpvis riktas mot svenska mål, utan någon särskild mottagare.

I *punkten 3* görs lagen även tillämplig på brott som begås eller kommer att begås med hjälp av informationssystem som finns i Sverige. Genom det kommer myndigheterna att kunna ingripa mot brott och brottslighet där brottet begås med hjälp av ett informationssystem i Sverige, oberoende av om någon gärningsman befinner i Sverige eller inte och oavsett om målet för brottet finns i ett annat land. Det kan vara fråga om att någon i ett annat land utnyttjar informationssystem eller servrar som finns i Sverige för ett cyberangrepp mot ett mål i ett tredje land. Det kan röra sig om informationssystem som finns i hallar med servrar som ägs eller används av personer eller företag i Sverige eller annan elektronisk utrustning i Sverige som är uppkopplad mot internet och som används som hjälpmedel för att begå brott eller som utnyttjas i brottslig verksamhet. Ett typiskt exempel är noder som ingår i ett anonymiseringsnätverk där det informationssystem som angriparen använder sig av finns utomlands eller det är okänt var det finns. Punkten 3 kompletterar således punkten 2 i den delen.

Förutsättningarna för ingripanden

3 §

Paragrafen reglerar, tillsammans med 4 och 5 §§, förutsättningarna för olika former av ingripanden i cybermiljö. Den har behandlats i avsnitt 14.2, 14.5 och 14.6.

I paragrafen räknas upp vilka åtgärder som Polismyndigheten, Säkerhetspolisen respektive Tullverket får vidta efter ett beslut enligt 11 § om ingripande. Uppräkningen är uttömmande.

Ett syfte med ingripanden är att förhindra brott i cybermiljö innan de begås. Det innebär att handlingen som konstituerar brottet inte ska ha kommit så långt att den kan bedömas som stämpling, förberedelse eller försök till brott. Ingripandet kan t.ex. utgå från underrättelseinformation eller andra omständigheter som ger ett objektivt underlag för bedömningen att ett visst brott ska påbörjas eller planeras. Det räcker däremot inte med allmänna antaganden eller med spekulationer om att så är fallet, utan det krävs någon faktisk omständighet som ger stöd för det. Vad som avses med brott och brottslig verksamhet och kopplingen till cybermiljö, framgår av kommentaren till 1 §.

Ett ingripande för att förhindra brott kan rikta sig mot en pågående brottsserie, t.ex. bedrägerier som med hjälp av digital teknik, på ett likartat sätt och under samma tidsperiod, begås mot en mängd personer. Ett annat exempel kan vara att hindra slumpvis utsända meddelanden som lockar mottagarna att klicka på länkar med skadlig programvara eller som förmår dem att avslöja inloggningsuppgifter som kan användas för brott. Det kan också handla om att hejda försäljning av narkotika via en marknadsplats på internet, där framtida köp av narkotika förhindras genom ingripande mot marknadsplatsen. I de nämnda fallen kan det ha förekommit fullbordade brott, men syftet med ingripandet är att förhindra att nya brott begås.

Ett annat syfte med ingripanden är att avbryta påbörjade brott i cybermiljö. Det kan röra sig om situationer där det finns förutsättningar att inleda förundersökning om konkreta brott i form av förberedelse, stämpling eller försök till brott i cybermiljö. Mot bakgrund av att viss brottslighet är systematisk och bedrivs mer eller mindre kontinuerligt, t.ex. narkotikaförsäljning på Darknet, kan det förutses att det vid ett planerat ingripande förekommer brottsligt handlande i olika stadier av fullbordan. Ett ingripande kan, beroende på vilken underrättelseinformation som finns och hur tillförlitlig den är, i sådana fall göras både i ett relativt tidigt skede, så snart det är fråga om ett handlande som kan utgöra straffbar planering eller förberedelse, eller vid ett nära förestående konkret brott.

Det finns också situationer där det saknas kunskap om huruvida brott har begåtts eller om det pågår endast icke straffbar planering

av framtida brottslig verksamhet, men där det samtidigt är viktigt att polisen kan avbryta agerandet så snart som möjligt. Ett exempel är att det upptäcks att en person på ett forum på internet erbjuder sig att tillverka skjutvapen på beställning eller att tillhandahålla någon annan kriminaliserad tjänst. Det kan även vara fråga om systematiska bedrägerier, där det är okänt om något brott har fullbordats men det sannolikt bara är en tidsfråga. Ingripandet ska syfta till att brottet eller brotten inte ska fullbordas.

Ett ytterligare syfte med ingripanden är att störa eller avbryta brottslig verksamhet i cybermiljö. Det kan finnas underrättelseinformation som tyder på att det pågår viss brottslig verksamhet (som innefattar en eller flera kriminaliserade gärningar), men där alla omständigheter kring brottet eller brotten inte är kända. Ett typiskt exempel kan vara bedrägerier, där det finns underrättelseinformation, t.ex. annonser på internet, som tyder på att det förekommer investeringsbedrägerier, men där varken de som ligger bakom brotten, de enskilda brotten, målsägandena eller andra fakta som behövs för att urskilja ett konkret brott är kända. Ett annat exempel kan vara att någon varnas för ett kommande ransomwareangrepp och kan lämna tillräcklig information för att ett ingripande enligt lagen ska kunna riktas mot ett visst informationssystem.

Att störa eller avbryta brottslig verksamhet i cybermiljö kan bestå i olika åtgärder som försvårar den pågående verksamheten. En störning kan typiskt sett åstadkommas genom blockering (punkten 2), t.ex. genom ett överbelastningsangrepp eller annan blockering av tillgången till en viss hemsida som erbjuder försäljning av narkotika.

Exempel på situationer där ett ingripande kan bli aktuellt är om någon med hjälp av ett informationssystem, på ett sätt som tydligt riktar sig till svenska mottagare, försöker förmå personer att t.ex. göra investeringar i bluffverksamhet eller att föra över sina ekonomiska tillgångar till någon som saknar avsikt att hantera dem på det sätt som har avtalats. Det kan också vara fråga om sms, som uppges komma från en seriös avsändare, t.ex. en myndighet eller ett välkänt företag, som skickas till en bred krets, där mottagaren ombeds att klicka på en länk med skadlig programvara. Det behöver emellertid inte vara fråga om brott som riktar sig mot många personer. Även brott som riktas mot en enskild person, t.ex. sexuella handlingar som ett barn förmås att göra mot sig själv på internet, kan störas med stöd av paragrafen.

En förutsättning för ett ingripande är att det behövs, dvs. att syftet med att ingripa inte kan uppnås genom några andra, mindre inkräktande, åtgärder. Det är samma grundläggande förutsättning som gäller för ingripanden i den fysiska miljön.

Begreppet bereda sig tillgång till ett informationssystem innebär i detta sammanhang att en myndighet – oftast utan att den vars uppgifter är föremål för ingripandet vet om det – genom en teknisk åtgärd eller på något annat sätt skaffar sig tillgång till systemet och uppgifter i det, se kommentaren till 17 §.

Att bereda sig tillgång till ett informationssystem ska göras i något av de syften som anges i punkterna 1 och 2, dvs. för att kunna genomföra olika åtgärder i systemet. Vad som avses med ett informationssystem framgår av kommentaren till 2 §. Regleringen är tillämplig även om syftet kan uppnås utan att myndigheten bereder sig tillgång till informationssystemet, t.ex. vid ett överbelastningsangrepp.

Ett ingripande kan riktas mot en eller flera uppgifter i ett informationssystem. Alla typer av uppgifter omfattas, även dataprogram av olika slag. Det saknar betydelse var uppgifterna finns eller förvaras i systemet. Därmed innefattas också uppgifter som finns i en dators temporära minne. Även uppgifter som ger tillgång till informationssystemet, t.ex. användning av ett virtuellt privat nätverk, omfattas. Uppgifter under befordran till eller från informationssystemet omfattas däremot inte.

Ett ingripande får beslutas endast om det är av särskild vikt för att förhindra eller avbryta brott eller störa eller avbryta brottslig verksamhet i cybermiljö. Kravet på särskild vikt innebär att det ska finnas sakliga skäl för bedömningen att ingripandet får betydelse för att förhindra, störa eller avbryta brottsliga förehavanden i cybermiljö. Den information som finns tillgänglig ska alltså ge vid handen att en sådan effekt kan förväntas. Kravet på särskild vikt innefattar både ett kvalitetskrav på den effekt som ingripandet kan ge och ett krav på att åtgärden behövs i det enskilda fallet. Bedömningen får inte bygga enbart på spekulationer eller allmänna antaganden utan ska grundas på faktiska omständigheter.

Enligt *punkten 1* är ett syfte med att myndigheten bereder sig tillgång till ett informationssystem och till uppgifter i det att kunna ändra uppgifter som ger tillgång till eller behandlas i informationssystemet.

Att ändra innebär i första hand att något görs för att påverka uppgifter som redan behandlas i informationssystemet, t.ex. uppgifter på digitala plattformar och tjänster. Det kan också innebära att nya uppgifter förs in, i syfte att någon annan ska uteslutas från teknisk tillgång till ett visst informationssystem. Ett exempel är att lösenord ändras för att begränsa tillgången till uppgifterna, så att myndigheten tillfälligt kan ta över en webbplats, en server eller en plattform som används för kriminell aktivitet. Det kan även innebära att information tillfälligt krypteras i samma syfte.

Endast ändringar som innebär att den som äger eller använder informationssystemet tillfälligt avhänds rådigheten över systemet eller vissa uppgifter i det omfattas av begreppet ändra. Det innebär att myndigheten ska möjliggöra att den, vars uppgifter är föremål för ingripandet, kan återfå rådigheten över dem. Det kan göras genom att myndigheten t.ex. tar bort kryptering, tillhandahåller en kopia av uppgifterna i fråga eller ser till att den berörde genom att byta lösenord på nytt kan få tillgång till sina uppgifter.

Enligt den nu aktuella punkten får ett ingripande även bestå i att blockera uppgifter som ger tillgång till eller behandlas i informationssystemet. Med blockera avses åtgärder som innebär att uppgifter görs oåtkomliga eller hindras från att flöda normalt. Åtgärden kan bestå i hindrande eller spärrande åtgärder av olika slag, t.ex. överbelastningsangrepp, kryptering eller tillfällig nedstängning av en funktion, eller att införa eller sprida program som gör att uppgifterna blockeras. Även det fallet att en programkod förs in och fyller minnesutrymmet, så att uppgifterna inte kan nås eller kan lokaliseras, omfattas av regleringen. Ett ingripande kan även bestå av blockering av enheter som ingår i ett ransomewareangrepp eller blockering av tillgången till uppgifter som innehåller övergreppsmaterial eller information om hur olagliga droger eller vapen kan anskaffas. Det är inte nödvändigt att blockeringen samtidigt medför ett avbrott eller på annat sätt allvarligt hindrar systemets drift (se kommentaren till punkten 2).

Åtgärder som innebär att uppgifter i ett informationssystem blockeras är inte, till skillnad från att uppgifter raderas, av oåterkallelig karaktär. Blockering av uppgifter i ett informationssystem är därför en mindre ingripande åtgärd än radering. Blockering kan göras med hjälp av t.ex. en programkod som möjliggör att den berörde

senare kan återfå rådigheten över uppgifterna. Utgångspunkten är att minsta möjliga skada ska uppkomma vid ingripandet.

En åtgärd kan i vissa fall innebära både en ändring och en blockering. Ändring av lösenord och kryptering av uppgifter för att begränsa tillgången till informationssystemet är exempel på det.

Enligt *punkten 2* får myndigheten genom annan liknande åtgärd störa eller hindra användningen av uppgifter som behandlas i informationssystemet. Med annan liknande åtgärd avses en åtgärd som till sin art är jämförbar med att ändra eller blockera uppgifter i systemet.

Att störa eller hindra användningen tar sikte på åtgärder som påverkar informationssystemet så att uppgifterna som behandlas i det inte kan användas som vanligt. Åtgärderna kan innebära att driften av systemet störs, att uppgifterna i det inte kan användas på vanligt sätt eller att de inte skyddas och underhålls på normalt sätt.

Åtgärder som kan falla under punkten kan vara att mata in eller överföra uppgifter till respektive från informationssystemet, t.ex. att genom särskilda program skapa och sända så stora mängder information att mottagarens system kollapsar eller får kraftigt nedsatt funktion. En sådan åtgärd förutsätter inte att myndigheten bereder sig tillgång till informationssystemet.

En åtgärd som innebär att systemet störs, eller som hindrar användningen av de uppgifter som behandlas i systemet, kan innebära att tillgången till uppgifterna begränsas kraftigt, utan att möjligheterna att använda informationssystemet helt spolieras. Kravet i 18 § på att åtgärden inte får orsaka olägenhet eller skada utöver vad som är absolut nödvändigt innebär emellertid att skadlig programvara som orsakar mer än tillfällig skada normalt inte bör användas.

Ett ingripande ska enligt 7 § alltid vara proportionerligt och den minst ingripande åtgärden ska därför väljas. Det saknar däremot betydelse om störningen anses vara allvarlig eller inte i den mening som avses i 4 kap. 9 c § brottsbalken.

Myndigheten kan behöva använda flera av åtgärderna i punkterna 1 och 2. Det kan bero på att det som myndigheten vill uppnå med ingripandet kan uppnås bara genom flera olika åtgärder tillsammans, eller genom att flera åtgärder vidtas i olika steg.

I vissa fall kan ingripandet misslyckas, så att den förväntade effekten av en åtgärd inte realiseras. Ett nytt beslut om ingripande behöver då fattas, antingen för att myndigheten ska få vidta samma åtgärd igen eller en annan åtgärd.

Åtgärderna bör normalt avse en begränsad mängd uppgifter som behandlas i ett informationssystem eller en särskilt avgränsad del av systemet, t.ex. ett användarkonto till kommunikations- eller lagringstjänster eller enstaka hemsidor på en server. Ibland behöver dock åtgärder riktas mot uppgifter i ett helt informationssystem. Det torde främst bli aktuellt när åtgärder snabbt måste vidtas i fall där ingripandet brådskar på grund av akut risk för allvarliga samhällsskador.

Ändamålen i paragrafen är överlappande. En åtgärd enligt punkten 1 kan t.ex. både syfta till att störa brottslig verksamhet och att, genom störningen, förhindra att brott begås.

Ett ingripande får endast avse uppgifter i den eller de delar av informationssystemet som utnyttjas för brott eller i brottslig verksamhet av tillräcklig svårhetsgrad (se kommentaren till 6 §) och för de särskilt angivna syftena. Om ett beslut om ingripande avser flera åtgärder ska ändamålet med varje åtgärd vara uppfyllt.

4 §

Paragrafen reglerar, tillsammans med 3 och 5 §§, förutsättningarna för olika former av ingripanden i cybermiljö. Den har behandlats i avsnitt 14.3, 14.4 och 14.6.

Paragrafen innebär att Polismyndigheten, Säkerhetspolisen eller Tullverket, efter ett beslut om ingripande enligt 11 §, tillfälligt får bereda sig tillgång till trafikuppgifter under befordran till eller från ett informationssystem.

Med att bereda sig tillgång till avses detsamma som i 3 §, se kommentaren till den paragrafen. Genom kravet på att ingripandet ska vara tillfälligt säkerställs att ingripandet är kortvarigt.

Föremålet för ingripandet är trafikuppgifter under befordran till och från informationssystemet, dvs. endast metadata i form av uppgifter om t.ex. vilka som är avsändare och mottagare av meddelanden, information om router, tidpunkter för när uppgifterna befordras, mängden uppgifter som befordras och ip-nummer och ip-adresser. Paragrafen omfattar alltså inte tillgång till innehållet i trafiken. Inte heller omfattar regleringen lagrade uppgifter.

En förutsättning för ingripande är att det kan antas att informationssystemet utnyttjas i brottslig verksamhet i cybermiljö. Vad som

avses med begreppet brottslig verksamhet framgår av kommentaren till 1 §. Att det kan antas att informationssystemet utnyttjas i sådan verksamhet innebär att det är inte tillräckligt med allmänna antaganden och spekulationer, utan antagandet ska bygga på konkreta och objektivt verifierbara omständigheter. Uttrycket kan antas innebär ett relativt lågt beviskrav. Det kan röra sig om underrättelseinformation som pekar på att en eller flera servrar används eller kan komma att användas för att begå ett cyberangrepp. Att kunna bekräfta eller utesluta att så är fallet är ett nödvändigt första steg för att – i de fall där det faktiskt finns risk för brott – kunna vidta nödvändiga motåtgärder. Trafiken i ett anonymiseringsnätverk kan behöva spåras för att kunna bekräfta eller utesluta att ett visst informationssystem utnyttjas i nätverket. Åtgärden kan vara nödvändig även för att kunna kartlägga trafiken till och från ett sådant informationssystem som har bekräftats ingå i ett anonymiseringsnätverk som misstänks användas i brottsligt syfte, för att förhindra att brott begås med informationssystemet som verktyg.

Kravet på särskild vikt innebär att det på sakliga grunder kan bedömas att ingripandet skulle ha betydelse för att kunna kartlägga om det i den brottsliga verksamheten i cybermiljö förekommer kommunikation mellan informationssystemet i fråga och andra informationssystem. Se kommentaren till 3 § om vad som avses med särskild vikt. Det kan röra sig om informationssystem i form av s.k. noder som ingår i anonymiseringsnätverk, t.ex. webbkameror eller wifiroutrar, eller servrar som finns i olika länder som ingår i kriminell digital infrastruktur.

Genom att kartlägga sådan kommunikation kan myndigheterna nysta upp ett anonymiseringsnätverk som används för illegala syften eller upptäcka tidigare okända servrar som ingår i kriminell digital infrastruktur eller som utnyttjas av främmande makt. Ingripandet syftar alltså inte till att löpande följa trafiken till och från informationssystemet, utan enbart till att – genom ett kortvarigt ingripande – kunna upptäcka vilken roll det kan ha eller ha haft i nätverket. Om det vid kartläggningen kan konstateras att ett visst informationssystem ingår eller har ingått i ett anonymiseringsnätverk kan det i enskilda fall finnas förutsättningar för att använda preventiva tvångsmedel för att utreda frågan vidare. Det kan också innebära att det finns grund för att vidta andra åtgärder enligt lagen, t.ex. att blockera

tillgången till ett eller flera informationssystem eller att radera en skadlig kod.

5 §

Paragrafen reglerar, tillsammans med 3 och 4 §§, förutsättningarna för ingripanden i cybermiljö i form av radering och har behandlats i avsnitt 14.5.

För att Polismyndigheten, Säkerhetspolisen och Tullverket ska få radera uppgifter i cybermiljö krävs att ett sådant beslut har fattats enligt 12 § eller, om det är fråga om ett intermistiskt beslut, enligt 13 §.

Se kommentaren till 3 § när det gäller begreppen förhindra och avbryta brott.

Ett ingripande enligt förevarande paragraf förutsätter att åtgärden är av synnerlig vikt för att förhindra eller avbryta brott. Det innebär att det ställs betydligt högre krav för radering än för andra ingripanden enligt lagen. Med synnerlig vikt avses att det ska vara mycket svårt, eller rent av omöjligt, att åstadkomma samma resultat genom någon annan åtgärd. Det innebär att bestämmelsen ska tillämpas restriktivt. Radering aktualiseras först när andra, mindre ingripande, åtgärder, t.ex. blockering, inte är tillräckliga. Radering av bilder från kränkande fotografering kan i vissa fall vara den enda åtgärd som är möjligt att vidta för att förhindra att bilderna sprids. En mindre ingripande åtgärd kan vara att blockera tillgången för utomstående till en marknadsplats där det bedrivs brottslig verksamhet, och därigenom förhindra fortsatt brottslighet, i stället för att radera uppgifterna på marknadsplatsen. Så länge de som står bakom marknadsplatsen inte har identifierats och bevismaterial som kan användas för lagföring har säkrats, kan blockering vara en lämpligare åtgärd än radering.

Avgörande för om åtgärden är av synnerlig vikt bör vara hur stor skada som brottet eller den brottsliga verksamheten kan orsaka om uppgifterna inte raderas. Hänsyn ska också tas till vilka uppgifter som det är fråga om. Radering aktualiseras i såväl situationer där nya brott i cybermiljö kan förhindras som där pågående brott i cybermiljö kan avbrytas. Radering bör dock vara en sista åtgärd, om någon annan åtgärd inte är tillräcklig.

Även omfattningen av det som ska raderas har betydelse, både för frågan om åtgärden i sig är proportionerlig och för frågan om hela eller delar av informationen kan hanteras på ett mindre ingripande sätt. Radering kan röra allt från tusentals filer eller bilder till någon enstaka bild eller film.

Radering kan avse såväl uppgifter i informationssystem som programvara. Lagrade uppgifter, t.ex. information på delar av digitala plattformar och tjänster, får raderas. Endast sådana uppgifter som myndigheten har fått tillgång till genom tillämpning av lagen får raderas. Det innebär att paragrafen inte är tillämplig på uppgifter som finns i en dator eller annan kommunikationsutrustning som myndigheten t.ex. har fått tillgång till genom beslag. Om samma information finns både på den beslagtagna enheten och på en lagringstjänst kan dock radering på den sistnämnda platsen komma i fråga.

Att radera uppgifter i ett informationssystem är – till skillnad från att blockera uppgifter – en åtgärd av oåterkallelig karaktär. Det saknar betydelse om uppgifterna även finns i andra informationssystem eller om det finns kopior av dem i fysisk form. Det är endast uppgifterna som ingripandet avser som ska hanteras så att de inte kan återställas i det aktuella informationssystemet för att åtgärden ska utgöra radering enligt lagen.

Byte av lösenord, i syfte att myndigheten ska kunna bereda sig tillgång till uppgifter som behandlas i ett informationssystem, är inte att betrakta som radering i lagens mening, eftersom den som tillfälligt genom lösenordsbytet berövas rådigheten över systemet har möjlighet att senare, genom ett nytt lösenordsbyte, återfå rådigheten och antingen återanvända det gamla lösenordet eller skapa ett nytt.

Ju fler uppgifter som raderas, desto mer ingripande får åtgärden som utgångspunkt anses vara. Radering av uppgifter som har ett tydligt illegitimt syfte, t.ex. en skadlig kod eller en hemsida som enbart bjuder ut förbjudna preparat eller föremål, är normalt sett mindre ingripande än radering av uppgifter som även kan ha ett normalt och legitimt syfte.

6 §

I paragrafen regleras hur allvarliga brott eller vilken brottslighet som krävs för att lagen ska vara tillämplig. Den har behandlats i avsnitt 14.6.

För att ingripanden enligt lagen ska vara tillåtna krävs att det är föreskrivet fängelse i ett år eller mer för brottet eller det brott som brottsligheten innefattar. Det innebär att åtminstone maximistraffet för brottet ska uppgå till ett års fängelse. Om den brottsliga verksamheten, eller det enskilda brottet, bedöms utgöra ringa brott kan det, beroende på straffskalan för brottet, innebära att det brottsliga handlandet inte uppfyller kravet på tillräcklig svårhetsgrad.

Det krävs vidare att brottet eller den brottsliga verksamheten har koppling till cybermiljö genom att brottet begås eller kommer att begås i den miljön eller att den brottsliga verksamheten bedrivs i den miljön med hjälp av informationssystem, se kommentaren till 1 §. Vad som avses med att brott begås eller kommer att begås framgår av kommentaren till 2 §.

Proportionalitet

7 §

Paragrafen reglerar proportionalitetsprincipen vid ingripanden i cybermiljö och har behandlats i avsnitt 14.7.

Proportionalitetsprincipen innebär att en åtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till motstående intressen. Skälen som talar för ett ingripande ska alltid vägas mot det intrång eller men som åtgärden innebär. Om ingripandet kan förväntas innebära allvarliga skador på ett informationssystem, eller skada personer eller egendom på annat sätt, kan avvägningen leda till att någon annan åtgärd bör användas, eller till att beslutsfattaren bör avstå från ingripande.

Allvaret i det brott eller den brottsliga verksamhet som ingripandet rör bör vara avgörande för bedömningen av om skälen för åtgärden uppväger det intrång eller men i övrigt som ingripandet innebär. Av stor vikt är också hur stort intrång i den personliga integriteten eller hur stor skada eller annat men som brottet eller den brottsliga verksamheten kan komma att orsaka om något ingripande inte görs.

Det minst inkräktande sättet att genomföra ingripandet ska som utgångspunkt användas. Endast om en viss åtgärd inte är tillräcklig för att uppnå den avsedda effekten, får mer ingripande åtgärder användas.

Ingripanden som riktar sig mot informationssystem och uppgifter som enbart har ett olagligt syfte, t.ex. en skadlig kod eller en hemsida som bjuder ut förbjudna preparat eller föremål, är som utgångspunkt oftare proportionerliga än ingripanden mot något som har ett normalt och legitimt syfte. Det kan också ha betydelse om ingripandet omfattar en eller flera typer av åtgärder. Vidare ska hänsyn tas till vilken eventuell skada som ingripandet kan leda till och om skadan är oåterkallelig. Vid proportionalitetsbedömningen ska hänsyn även tas till om ingripandet riktar sig mot informationssystem med få eller många användare och hur ingripandet kan begränsas. Ingripanden som riskerar att få inverkan på många informationssystem eller många användare förutsätter att det är fråga om synnerligen allvarlig brottslighet för att de ska vara proportionerliga.

Mot bakgrund av det högre krav som enligt 5 § gäller för radering, att åtgärden är av synnerlig vikt, ligger det i sakens natur att radering i färre situationer kan anses vara proportionerlig.

När åklagaren prövar frågan om radering ska han eller hon, inom ramen för proportionalitetsbedömningen, även beakta att radering kan utgöra ett mindre integritetsintrång för den som äger eller använder det informationssystem som ingripandet avser än för den som blir utsatt för brott i cybermiljö. Det kan exempelvis gälla övergreppsmaterial eller känsliga personuppgifter som har stulits.

Proportionalitetsprincipen får även betydelse för hur beslut om ingripande bör utformas och vilka villkor som bör gälla för sådana beslut. Kravet på proportionalitet gäller även när ingripandet genomförs och ska därför beaktas självmant av den som genomför ingripandet; t.ex. kan integritetsintrånget bli så stort att ingripandet inte längre kan anses vara proportionerligt.

Förbud mot att ingripa

8 §

I paragrafen föreskrivs förbud mot att rikta ingripanden enligt lagen mot dels vissa informationssystem, dels vissa uppgifter. Paragrafen har behandlats i avsnitt 15.2.

Det *första stycket* består av två punkter, som klargör att det finns ett absolut förbud mot att ingripa i cybermiljö mot vissa informationssystem. För båda punkterna gäller att informationssystemet stadigvarande ska användas eller vara särskilt avsett att användas i viss verksamhet.

För att informationssystemet ska ha den priviligierade ställningen krävs att det är en bestående del av verksamheten och används i något av de angivna syftena eller att det är särskilt avsett att användas i verksamheten. En dator, mobiltelefon eller liknande kommunikationsutrustning, som stadigvarande används i verksamheterna i fråga, är enligt bestämmelsen fredad från ingripanden enligt lagen. Det är däremot inte möjligt att undgå ett ingripande i cybermiljö genom att tillfälligt använda ett informationssystem i sådan verksamhet som avses i paragrafen.

Regleringen innebär inte att internetbaserade elektroniska tjänster, som det går att få tillgång till från utrustningen, automatiskt är fredade från ingripanden. Exempelvis kan ett ingripande i cybermiljö avse en präst privata konto i sociala medier eller privata internetbaserade e-post, även om prästen uteslutande använder sin tjänstedator för att logga in på sådana tjänster.

Förbuden gäller inte heller för privata mobiltelefoner eller datorer som tillhör någon av de i paragrafen avsedda yrkeskategorierna, även om utrustningen vid enstaka tillfällen också används i sådan verksamhet som har särskilt skydd.

Informationssystem som endast tillfälligt används i verksamheten eller är till för personer utanför verksamheten, t.ex. besöksdatorer i en fredad verksamhet, omfattas inte heller av förbuden.

Ett informationssystem som är särskilt avsett att användas i verksamheten kan t.ex. vara ett system som innehas av en frilansande journalist som ännu inte har startat sin verksamhet, men som har tagit med sig arbetsrelaterad information från en tidigare arbetsgivare och lagrat den i systemet.

Eftersom förbudet tar sikte på informationssystemet som sådant och inte den plats där det finns, är den fysiska arbetsplatsen för de berörda yrkeskategorierna av mindre betydelse. Det avgörande är om informationssystemet stadigvarande används eller är särskilt avsett att användas i de angivna verksamheterna. Det innebär t.ex. att en dator eller mobiltelefon, som stadigvarande används för fredad verksamhet, i vissa fall kan vara oåtkomlig.

Punkten 1 rör verksamheter där tystnadsplikt gäller enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL. Här avses primärt medieföretag, t.ex. tidningar, förlag eller nyhetsbyråer, som bedriver verksamhet för vilken det råder tystnadsplikt enligt reglerna i TF eller YGL.

Det finns undantag från tystnadsplikten i 3 kap. 4 § TF och 2 kap. 4 § YGL. Vidare kan den till vars förmån tystnadsplikten gäller lämna sitt medgivande till att den bryts. Om ett undantag gäller finns det inget som hindrar att ett ingripande i cybermiljö görs, under förutsättning att det inte inkräktar på tystnadsplikt till förmån för någon annan.

Punkten 2 tar sikte på informationssystem som används av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund. Tystnadsplikten som gäller för den yrkeskategorin är absolut. Det finns alltså inga undantag från den. Punkten avser emellertid endast informationssystem som används i verksamhet för bikt eller enskild själavård. Förbudet omfattar informationssystem som används i sådan verksamhet som bedrivs i t.ex. kyrkor, synagogor och moskéer. Förbudet gäller emellertid inte enbart på grund av att ett informationssystem används på en sådan plats. Det ska vara fråga om informationssystem som stadigvarande används eller är särskilt avsedda att användas i verksamhet för bikt eller själavård. Ytterst blir det en fråga i varje enskilt fall att bedöma om ett ingripande enligt lagen är tillåtet.

Regleringen i *andra stycket* tar sikte på uppgifter som har anförtrotts bl.a. advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter och familjerådgivare enligt socialtjänstlagen (2025:400) samt rättegångsombud, deras biträden och försvarare som inte är advokater i deras yrkesutövning eller som de erfarit i samband med den. Det innebär att ingripanden i cybermiljö inte får avse t.ex. digitala journalsystem hos läkare, tandläkare och annan sjukvårdspersonal eller digital klientinformation hos en advokat eller en familjerådgivare hos socialtjänst.

Begreppet advokat innefattar i detta sammanhang även den som är auktoriserad som advokat i någon annan medlemsstat i EU, Europeiska ekonomiska samarbetsområdet eller i Schweiz, när han eller hon är verksam i Sverige (8 kap. 9 § RB).

Det är i och för sig inget som hindrar att myndigheten bereder sig tillgång till ett informationssystem som används av någon i de skyddade yrkeskategorierna, under förutsättning att ingripandet inte avser uppgifter som personen har anförtrotts i sin yrkesutövning och som han eller hon inte får höras som vittne om. Skyddet avser uppgifter i informationssystem som används, privat eller i tjänsten, av någon av de nämnda yrkeskategorierna och som innehåller uppgifter som inte får röjas på grund av tystnadsplikten. Det avgörande är alltså inte hur eller av vem informationssystemet används utan uppgifterna som sådana.

I 36 kap. 5 § fjärde stycket RB regleras undantag från tystnadsplikten för nyss nämnda yrkeskategorier vid mycket allvarliga brott. Undantagen gäller dock inte för försvarare. Vidare kan den till vars förmån tystnadsplikten gäller lämna sitt medgivande till att den bryts. Om ett undantag gäller finns det inget som hindrar att ett ingripande enligt lagen görs, så länge det inte inkräktar på tystnadsplikt till förmån för någon annan.

Enligt *tredje stycket* ska åtgärden omedelbart avbrytas om det vid ett ingripande i cybermiljö visar sig att ingripandet riktar sig mot ett informationssystem, som omfattas av förbud enligt första stycket, eller mot uppgifter som omfattas av förbud enligt andra stycket. I praktiken torde det i de flesta fall vara först när myndigheten har berett sig tillgång till ett informationssystem och tar del av uppgifter i det som det upptäcks att det kan vara fråga om sådan information som omfattas av förbud. Så fort det står klart att så är fallet ska ingripandet avbrytas i den del som det omfattas av förbud.

Lagen tillåter inte att myndigheten hämtar in uppgifter genom att t.ex. kopiera dem eller på annat sätt föra över dem till ett eget informationssystem, om det inte är ett absolut nödvändigt tekniskt steg för att kunna genomföra någon del av ingripandet. Om det ändå skulle göras, t.ex. på grund av ett misstag från myndighetens sida, ska eventuell information som myndigheten har fått tillgång till och som omfattas av förbud förstöras omedelbart. Minnesanteckningar eller liknande som myndigheten för i samband med ingripandet om-

fattas emellertid inte av förbudet, så länge de inte återger uppgifter som myndigheten är förbjuden att ta del av.

Beslut om tillträde

9 §

I paragrafen anges förutsättningarna för att fatta ett särskilt beslut om tillträde till annars skyddade platser. Ett beslut om tillträde avser, i motsats till ett beslut om ingripande i ett informationssystem, en fysisk plats. Paragrafen har behandlats i avsnitt 17.3.1.

Enligt *första stycket* får myndigheten, om det är nödvändigt för att genomföra ett ingripande enligt lagen, efter särskilt beslut, bereda sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Med tekniskt hjälpmedel avses både hårdvara och programvara. Regleringen förutsätter att installationen ska göras på plats. Den ger alltså inte myndigheten någon rätt att ta med sig informationssystemet därifrån.

Beslut om tillträde krävs främst för platser som skyddas genom bestämmelserna i 4 kap. 6 § brottsbalken om hemfridsbrott och olaga intrång. Skyddet gäller inte bara för bostäder utan också för bl.a. arbetsplatser, föreningslokaler och bilar. Ett beslut om tillträde behövs också för tillträde till en plats som skyddas genom bestämmelsen i 8 kap. 8 § brottsbalken om egenmäktigt förfarande.

Tillträde till annars fredade platser kan i vissa fall ordnas genom att den som förfogar över platsen ger sitt samtycke. Då behövs inget beslut om tillträde. Vidare kan ingripandet i vissa fall göras öppet, på samma sätt som t.ex. en husrannsakan. Regleringen medger dock att myndigheten även bereder sig tillträde i hemlighet i de undantagsfall där det bedöms vara nödvändigt.

Ett beslut om tillträde ger den ingripande myndigheten bl.a. rätt att bryta lås eller på något annat sätt rubba någons egendom, t.ex. att öppna en låst väska där det finns särskild anledning att anta att det eftersökta informationssystemet finns. Myndigheten får ta sig in i det skyddade utrymmet med våld. Den får alltså – om det är nödvändigt – bryta eller dyrka sig in i en bostad eller ett annat utrymme som omfattas av beslutet för att genomföra installationen (eller avinstallationen, se kommentaren till 19 §). Ett beslut om tillträde innefattar en befogenhet att tillfälligt sätta larmanordningar ur funktion.

Enligt *andra stycket* får beslut om tillträde endast avse en plats där det finns särskild anledning att anta att informationssystemet finns tillgängligt. Kravet på att informationssystemet ska vara tillgängligt innebär inte att det behöver finnas fysiskt tillgängligt på den plats där tillträdet äger rum. Det kan i vissa fall vara så att det tekniska hjälpmedlet kan installeras på distans. Det följer av proportionalitetsprincipen att den minst integritetskänsliga platsen ska väljas i första hand. Ett ingripande i cybermiljö kan i vissa fall göras genom ingrepp i en kopplingsstation men avse uppgifter i ett informationssystem i en annan del av huset eller i ett annat hus. Beslut om tillträde bör i så fall kunna beviljas för att fysiskt få tillträde till kopplingsstationen.

Kravet på att det ska finnas särskild anledning att anta att informationssystemet finns tillgängligt på den plats som beslutet om tillträde avser innebär att det ska finnas någon faktisk omständighet som med viss styrka talar för att informationssystemet kommer att finnas där i vart fall någon gång under den tid som ingripandet får genomföras. Det räcker alltså inte med ett allmänt antagande om att informationssystemet kommer att finnas på platsen.

Om platsen för beslutet om tillträde är någons stadigvarande bostad ställs högre krav. Enligt *andra stycket* får beslut fattas endast om det finns synnerlig anledning att anta att informationssystemet finns tillgängligt där. Med synnerlig anledning avses att det ska vara så gott som säkert att informationssystemet finns tillgängligt i bostaden i fråga. Det högre kravet gäller endast för bostäder som används stadigvarande. Det gäller alltså inte tillfälliga bostäder, som hotellrum eller tillfälliga sovarrangemang i t.ex. möteslokaler eller andra liknande platser.

Beslut om tillträde får fattas av särskilda befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket eller av åklagare, dvs. av dem som fattar beslut enligt lagen. Det ska framgå av beslutet om ingripande att ett beslut om tillträde har fattats. I beslutet ska platsen för tillträde anges (se kommentaren till 16 §). Ett beslut om tillträde gäller för hela den tid som ingripandet får genomföras (om inte något annat anges i beslutet, se kommentaren till 16 §) och även efter utgången av den tiden till såvitt avser borttagande eller avinstallation av tekniska hjälpmedel (se 19 §). Frågan om beslut om tillträde ska alltid bedömas fristående från beslut om att ingripa.

10 §

I paragrafen regleras vilka platser som alltid är fredade mot tillträde enligt 9 §. Den har behandlats i avsnitt 17.3.2.

Enligt paragrafen får ett beslut om tillträde aldrig avse platser som stadigvarande används eller är särskilt avsedda att användas för vissa verksamheter. Vilka de verksamheterna är anges i tre punkter. *Punkterna 1* och *3* är desamma som de som anges i 8 § första och tredje styckena (se kommentaren till den paragrafen). I punkten 2 skyddas sådan verksamhet som bedrivs av vissa av de yrkeskategorier som anges i 8 § andra stycket.

Kravet på att en plats stadigvarande används eller är särskilt avsedd att användas för det fredade ändamålet medför att det inte är möjligt att undvika ett beslut om tillträde endast genom att tillfälligt upplåta eller inrätta en lokal för sådan verksamhet.

Beslut om ingripanden

11 §

I paragrafen regleras vem som får besluta om samtliga åtgärder förutom radering. Paragrafen har behandlats i avsnitt 16.1.

Befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket får fatta beslut om ingripanden enligt 3 §, dvs. beslut om att bereda sig tillgång till informationssystem och uppgifter i det i syfte att ändra eller blockera uppgifter som ger tillgång till eller behandlas i systemet eller genom någon annan liknande åtgärd tillfälligt störa eller hindra användningen av uppgifter som behandlas i systemet. Detsamma gäller beslut enligt 4 § för att kartlägga om det i brottslig verksamhet förekommer kommunikation mellan informationssystem. Beslut får fattas endast av särskilt utsedda befattningshavare. Vilka krav som ställs på befattningshavaren regleras i förordning.

Befattningshavaren får, i anslutning till att ett beslut enligt 3 eller 4 § fattas, även besluta om tillträde enligt 9 §. Det finns dock inget som hindrar att ett beslut om tillträde fattas senare, om det först då blir tydligt att ett sådant beslut behövs.

12 §

I paragrafen regleras dels vem som får besluta om radering, dels vem som får initiera frågor om radering. Paragrafen har behandlats i avsnitt 16.2.1.

Enligt paragrafen ska åklagare besluta om radering enligt 5 §. Det kan, om inte riksåklagaren beslutar annat, vara åklagare vid såväl Åklagarmyndigheten som Ekobrottsmyndigheten.

Ansökan om radering ska göras av Polismyndigheten, Säkerhetspolisen respektive Tullverket. En ansökan om radering ska vara skriftlig och innehålla all den information som åklagaren behöver för att kunna ta ställning i frågan. Det innebär att det bör framgå av ansökan bl.a. vad syftet med raderingen är, vilka uppgifter som ska raderas, i vilket informationssystem (eller vilken del av ett informationssystem) som uppgifterna som ska raderas finns och hur raderingen ska genomföras, om åklagaren beslutar om det.

När åklagaren prövar frågan om radering, bör han eller hon överväga om radering kan få konsekvenser för eventuell framtida brottsutredning och lagföring av det brott som ligger bakom ingripandet eller för någon annan brottsutredning.

Åklagaren får i samband med ett beslut om radering även besluta i fråga om tillträde enligt 9 §.

13 §

Paragrafen reglerar förutsättningarna för att interimistiskt besluta om radering och, i förekommande fall, om tillträde i samband med det. Den innehåller också bestämmelser om det fortsatta förfarandet när interimistiska beslut har fattats. Paragrafen har behandlats i avsnitt 16.2.2.

Ett interimistiskt beslut om radering får enligt *första stycket* fattas av en särskilt utsedd befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket, se kommentaren till 11 §.

En grundläggande förutsättning för att ett beslut om radering ska få fattas av annan än åklagare är att det är fråga om förestående brott som skulle kunna förhindras eller om pågående brott som behöver avbrytas genom raderingen. På det sättet markeras att interimistiska beslut ska fattas restriktivt och att tillämpningsområdet för paragrafen är snävare än det som gäller enligt 5 §.

Vidare krävs att det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för möjligheterna att ingripa att inhämta åklagarens beslut. Det innebär att det endast är i situationer där ingripandena är så brådskande att syftet med ingripandet riskerar att gå förlorat om det inte genomförs omedelbart som interimistiska beslut får fattas. Se kommentaren till 5 § angående situationer där radering kan aktualiseras. Som nyss nämnts är dock tillämpningsområdet enligt förevarande paragraf snävare.

Det gäller samma formella krav för ett interimistiskt beslut om radering som för ett åklagarbeslut om radering. Beslutsfattaren har i förekommande fall möjlighet att förena ett interimistiskt beslut om radering med ett beslut om tillträde enligt 9 §.

När ett interimistiskt beslut om radering har fattats ska enligt *andra stycket* beslutsfattaren så snart som möjligt anmäla det till åklagare. Att anmälan ska göras så snart som möjligt innebär att den ska göras så snart någon behörig person på åklagarmyndigheten kan ta emot den. Eftersom det får förutsättas att endast vissa åklagare kommer att handlägga frågor enligt lagen innebär det att anmälan inte behöver hanteras av andra åklagare under jour och beredskap.

Anmälan ska vara skriftlig och ange skälen för beslutet. Om det har funnits tid att fatta ett skriftligt interimistiskt beslut om radering kan det utgöra anmälan, om uppgifterna i beslutet är tillräckliga för att uppfylla kraven i förevarande paragraf.

Om möjligt ska en kopia av de uppgifter som har raderats eller ska raderas fogas till anmälan, för att åklagaren ska kunna bedöma om beslutet är lagligen grundat. Om de raderade uppgifterna inte finns tillgängliga för den ingripande myndigheten antingen i form av en kopia i något annat informationssystem än det som ingripandet har riktats mot, eller i fysisk form, ska myndigheten, om det är tekniskt möjligt, bevara en kopia av de uppgifter som det intermistiska beslutet avser. Om det inte är tekniskt möjligt att göra och bevara en sådan kopia, eller om en sådan åtgärd skulle riskera att avslöja arbetsmetoder som omfattas av sekretess, bör det på annat sätt dokumenteras vilka uppgifter som avses.

14 §

I paragrafen regleras åklagares prövning av interimistiska beslut om radering och eventuella beslut om tillträde och det fortsatta förfarandet vid den prövningen. Paragrafen har behandlats i avsnitt 16.2.2. och 16.2.3.

Enligt *första stycket* ska åklagaren, när han eller hon underrättas, så snart som möjligt pröva om det finns skäl för radering och ett eventuellt beslut om tillträde som har fattats i anslutning till det. Kravet på att beslutet ska prövas så snart som möjligt innebär att åklagaren inte får skjuta upp prövningen. Prövningen behöver dock inte göras under jour och beredskap av åklagare som inte normalt handlägger ärenden enligt lagen.

Åklagaren ska pröva beslutet på samma sätt som vid en ansökan om radering. Även om åklagaren konstaterar att det i och för sig saknades skäl för det interimistiska beslutet när det beslutades, men det har tillkommit nya omständigheter, kan det utmynna i att det finns skäl för ingripande. Om åklagaren däremot bedömer att det inte finns skäl för radering, ska han eller hon omedelbart upphäva beslutet, om raderingen inte redan har genomförts. Pågår raderingen ska åtgärden genast avbrytas.

Har raderingen redan genomförts när åklagaren prövar det interimistiska beslutet, ska åklagaren enligt *andra stycket* underrätta Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd om det interimistiska beslutet och sitt ställningstagande, i stället för att upphäva beslutet. Det inkluderar eventuellt beslut om tillträde som har fattats i samband med ett intermistiskt beslut om radering. Vad en sådan underrättelse bör innehålla regleras i förordning.

I de fall där åklagaren finner att det har saknats skäl för radering som har genomförts ska åklagaren också underrätta den vars uppgifter har raderats, om han eller hon är känd, om sitt ställningstagande. Om de raderade uppgifterna har kopierats, ska åklagaren upplysa den vars uppgifter har raderats om att han eller hon har möjlighet att begära hos den ingripande myndigheten att få en kopia av det som har raderats.

Enligt *tredje stycket* ska åklagaren säkerställa att kopior av raderade uppgifter förstörs senast sex månader efter prövningen. Kopiorna bör bevaras en viss tid bl.a. för att möjliggöra tillsyn. Regleringen

innebär ett undantag från de generella bestämmelserna om gallring av allmänna handlingar. Gallring förutsätter enligt 14 § arkivförordningen (1991:446) beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning. Tredje stycket utgör sådant lagstöd som krävs för förstöring. Om ett ingripande i cybermiljö resulterar i en förundersökning och en kopia av uppgifterna av det skälet tas in i ett förundersökningsprotokoll, ska kopian dock bevaras enligt de regler som gäller för bevarande av förundersökningsprotokoll.

Åklagaren kan, på samma sätt som vid förstöring av material från hemliga tvångsmedel, uppdra åt någon annan att genomföra förstöringen.

Villkor

15 §

Paragrafen reglerar villkor i beslut om ingripande enligt lagen. Den har behandlats i avsnitt 17.2.

Utgångspunkten är att ingripanden ska begränsas genom villkor, för att säkerställa att enskildas integritet inte kränks i onödan, när det är möjligt och lämpligt.

Villkor kan ta sikte på i stort sett vilka omständigheter som helst som kan gagna skyddet för den personliga integriteten. Villkoren kan t.ex. avse närmare föreskrifter om vilka delar av ett informationssystem som ingripandet får rikta sig mot. Villkoren kan även avse vilka uppgifter som den ingripande myndigheten får vidta åtgärder med, t.ex. endast lagrade uppgifter av viss filtyp, viss karaktär eller med viss beteckning.

Villkor kan i vissa fall vara obehövliga, t.ex. om myndigheten har vederhäftig information om att informationssystemet bara används i brottsligt syfte. Det kan vara fallet om ingripanden riktas mot t.ex. webbplatser på Darknet som förmedlar kriminella tjänster eller chattkonton som enbart används för kommunikation mellan kriminella. Ibland kan den omständigheten att informationssystemet endast har använts under en begränsad tid göra att villkor framstår som obehövligt. Vid utformningen av villkoren bör det beaktas att begränsande villkor kan försvåra genomförandet. En bedömning av om det finns

skäl för att ange villkor i ett beslut måste därför alltid göras i det enskilda fallet.

Innehållet i beslut

16 §

I paragrafen behandlas formkrav och vilka uppgifter som beslut om ingripanden i cybermiljö ska innehålla. Paragrafen har behandlats i avsnitt 17.1.

Av *första stycket* framgår att beslut om ingripanden ska vara skriftliga. Om det skulle medföra en fördröjning av väsentlig betydelse för syftet med ingripandet får beslutet dock fattas muntligen. Det finns nämligen situationer som kräver att beslut om ingripande fattas mycket snabbt, eftersom fördröjningen kan hindra eller försvåra att ingripandet görs. Beslutet ska i så fall dokumenteras så snart som möjligt. Dokumentationen av ett muntligt beslut ska ha samma innehåll som ett skriftligt beslut.

I *andra stycket* anges i sju punkter vilka uppgifter som ska anges i ett beslut.

Enligt *punkten 1* ska ändamålet med ingripandet anges. Ändamålen regleras i 3–5 §§. Som framgår av kommentaren till 3 § får ett ingripande endast avse uppgifter i den eller de delar av ett informationssystem som har samband med brott eller brottslig verksamhet av tillräcklig svårhetsgrad och för de särskilt angivna ändamålen. Om ett beslut avser flera åtgärder ska ändamålet med varje åtgärd anges.

Enligt *punkten 2* ska det anges vilket brott eller vilken brottslig verksamhet som ingripandet avser. Kravet på brottets svårhetsgrad regleras i 6 §.

Av *punkten 3* framgår att det också ska anges vilket informationssystem som ingripandet avser. Det betyder att det måste anges vilket specifikt informationssystem som beslutet gäller. Uppgifterna ska i vart fall vara så specificerade att det går att genomföra ingripandet och att det är möjligt att bedöma kopplingen mellan informationssystemet och ingripandet för att utesluta förväxlingsrisk med andra informationssystem. Det kan göras genom att exempelvis ett visst serienummer, IMEI-nummer, MAC-adress eller andra uppgifter som möjliggör identifiering av informationssystemet anges. Om det är möjligt ska det i beslutet anges vilken avgränsad del av informa-

tionssystemet som beslutet avser, exempelvis det användarkonto eller annan avgränsad del av tjänsten som ingripandet ska göras i. Det kan vara t.ex. en e-postadress eller ett användarnamn till ett konto på sociala medier eller annan internetbaserad tjänst.

Enligt *punkten 4* ska det vidare anges vilken åtgärd som ingripandet omfattar. Vilka åtgärder som ett ingripande kan omfatta regleras i 3–5 §§. Myndigheten kan ibland behöva använda flera av åtgärderna, eller flera åtgärder i olika steg, för att uppnå avsett resultat. Det ska då framgå av beslutet.

I vissa fall kan ingripandet misslyckas, på det sättet att den förväntade effekten av åtgärden inte realiseras. Ett nytt beslut om ingripande i form av samma eller en annan åtgärd kan då behöva fattas. Vidare kan ett nytt beslut behöva fattas om en åtgärd endast delvis leder till den avsedda effekten och därför behöver kompletteras med någon annan typ av åtgärd.

I *punkten 5* föreskrivs att det ska anges när ingripandet senast ska genomföras. När tiden bestäms ska begränsningen i andra stycket beaktas.

Enligt *punkten 6* ska det av beslutet framgå vilka villkor som gäller för ingripandet, se kommentaren till 15 § om villkor.

I *punkten 7* föreskrivs att det även ska anges om ett beslut om tillträde enligt 9 § har fattats och vilken plats det i så fall omfattar. Om beslutet om tillträde avser en bostad eller ett kontor ska adressen anges. Om beslutet däremot avser ett förvaringsskåp bland andra behöver inte det specifika skåpet pekas ut. Det räcker att det i beslutet anges att det avser ett förvaringsskåp i ett visst omklädningsrum eller liknande. Om beslutet avser en bil är det tillräckligt att fordonet individualiseras.

Ett beslut om ingripande kan avse flera informationssystem, t.ex. om det finns kopior av uppgifter som ska raderas i flera olika informationssystem.

Enligt *andra stycket* får tiden för att genomföra ingripandet inte bestämmas längre än nödvändigt. Att bereda sig tillgång till informationssystem kan vara tidskrävande, vilket måste beaktas när tiden bestäms. Även omfattningen av de uppgifter som ingripandet avser ska beaktas när tiden bestäms. Olika typer av åtgärder kräver olika lång tid att genomföra. Det är inte heller säkert att myndigheten på förhand har en klar bild över var uppgifterna finns i det informa-

tionssystem som ingripandet riktar sig mot. Då kan det behövas längre tid.

När beslutsfattaren bestämmer vad som är en nödvändig tidsram, bör hänsyn tas till både den tid som kan behövas för att installation av hjälpmedel eller motsvarande ska kunna utföras och att ingripandet ska kunna genomföras. I många fall kommer det att krävas viss tid för att förbereda genomförandet. Vissa förberedande åtgärder kommer inte att kunna göras innan beslut om ingripande har fattats.

En bortre tidsgräns gäller för genomförandet. Tiden får inte överstiga en månad från dagen för beslutet. Tidsgränsen avser den tid som får utnyttjas för genomförandet, inte den tid som själva ingripandet får ta.

Om det behövs längre tid för att genomföra ingripandet än en månad krävs det ett nytt beslut. Det krävs också ett nytt beslut om ett ingripande har gjorts, men det har misslyckats i den meningen att den brottsbekämpande myndigheten visserligen har kunnat bereda sig tillgång till informationssystemet men inte kunnat vidta de planerade åtgärderna i systemet. Det kan jämföras med att en husrannsakan görs, men att eftersökta föremål inte anträffas. Det krävs då ett nytt beslut om husrannsakan för att på nytt få leta efter samma föremål på samma plats. Ett misslyckande att bereda sig tillgång till informationssystemet innebär däremot inte att något nytt beslut krävs.

Hur ingripanden ska genomföras

17 §

I paragrafen regleras, tillsammans med 18 och 19 §§, hur ingripanden enligt lagen ska genomföras. Den har behandlats i avsnitt 18.1 och 18.2.

Enligt *första stycket* får beslut om ingripanden verkställas omedelbart. Snabbt genomförande torde i de flesta fall vara viktigt för att uppnå syftet med ett ingripande. I de fall där det är angeläget att avvakta med genomförandet finns det dock möjlighet till det. Ett exempel är att ingripandet behöver samordnas med någon annan brottsbekämpande åtgärd eller att det av något annat skäl finns anledning att välja en framtida tidpunkt för ingripandet.

I *andra stycket* regleras tillåtna tekniska metoder, dvs. hur myndigheten får bereda sig tillgång till ett informationssystem och uppgifter i det. När ett beslut om ingripande har fattats och ska genomföras får de tekniska hjälpmedel som behövs användas. Regleringen är teknikneutral för att inte begränsa den framtida teknikutvecklingen. Endast de tekniska hjälpmedel som behövs för att kunna genomföra ingripandet får dock användas. Med tekniska hjälpmedel avses här både hårdvara och mjukvara. Myndigheten bestämmer vilken teknik som ska användas i det enskilda fallet.

Regleringen tillåter att myndigheten bereder sig tillgång till informationssystem genom olika tekniska lösningar. Systemskydd får brytas eller kringgås och tekniska sårbarheter får utnyttjas. Att kringgå eller bryta systemskydd kan innebära att myndigheten genom avancerade tekniska åtgärder bereder sig tillgång till informationssystemet, t.ex. genom att installera ett program och på så sätt t.ex. ta sig förbi en multifaktorautentisering. Det kan även innebära att myndigheten bereder sig tillgång till informationssystemet på samma sätt som den normale användaren.

Att utnyttja sårbarheter i informationssystem innebär att myndigheten drar nytta av omständigheter som gör ett informationssystem känsligt för angrepp.

Regleringen utesluter inte att flera olika tekniker eller metoder används vid samma ingripande. Det aktsamhetskrav som föreskrivs i 18 § kan dock begränsa vilka tekniska hjälpmedel som får användas, se kommentaren till den paragrafen.

18 §

Paragrafen reglerar, tillsammans med 17 och 19 §§, hur ingripanden enligt lagen ska genomföras. I förevarande paragraf föreskrivs vilken aktsamhet som ska iakttas när ingripanden genomförs. Den har behandlats i avsnitt 18.3.

Paragrafen innehåller en generellt utformad aktsamhetsregel som alltid gäller när ingripanden enligt lagen ska genomföras. Den förbjuder inte att skada eller olägenhet uppstår, men föreskriver att den i så fall måste vara absolut nödvändig. Syftet med ingripandet har stor betydelse för bedömningen av om skadan eller olägenheten går utöver vad som är absolut nödvändigt, eftersom det direkta syftet

med en viss åtgärd, t.ex. blockering eller radering av uppgifter i informationssystemet, kan vara att orsaka skada eller olägenhet för den som äger eller använder informationssystemet. Genom proportionalitetsprincipen ställs det krav på att det minst ingripande sättet ska väljas om ingripandet kommer att innebära skada eller olägenhet för en person, t.ex. åverkan på någons dator eller mobiltelefon vid installation av hårdvara.

Regleringen har även betydelse i fråga om tillträde till den plats där ingripandet ska göras och på vilket sätt tekniska hjälpmedel ska installeras. Den är tillämplig på såväl fysisk miljö som cybermiljö där ingripanden enligt lagen genomförs.

Ingripanden ska genomföras på sådant sätt att påverkan på annan som använder samma del av informationssystemet blir så begränsad som möjligt. Det gäller särskilt om ett ingripande riktar sig mot servrar som har flera användare eller om ingripandet görs mot ett informationssystem som är tillgängligt för eller används av flera personer. Ingripanden kan också avse en begränsad del av ett större informationssystem, exempelvis ett användarkonto till en kommunikationstjänst, lagringstjänst eller annan internetbaserad tjänst som används av flera gemensamt för kommunikation eller lagring. Det kan uppstå situationer där inte samtliga användare av kontot kan knytas till det brott eller den brottsliga verksamhet som ingripandet avser. I sådana fall är det särskilt viktigt att myndigheten i möjlig mån begränsar den påverkan på andra personers användning av informationssystemet som ingripandet kan få.

Den nu aktuella begränsningen är dock inte avsedd att träffa ingripanden vilkas syfte är att direkt påverka andras användning av ett informationssystem som helt eller till stor del används för brottsliga ändamål. Det kan t.ex. vara fråga om att blockera tillgången till en marknadsplats för att förhindra försäljningen av olagliga varor eller att blockera tillgången till terrorisminnehåll för att förhindra bombtillverkning.

19 §

Paragrafen reglerar, tillsammans med 17 och 18 §§, hur ingripanden ska genomföras. I paragrafen föreskrivs vad som gäller när ingripandet har genomförts eller beslutet om ingripande har upphört att gälla. Paragrafen har behandlats i avsnitt 18.2.

I paragrafen regleras kravet på att de tekniska hjälpmedel som myndigheten har installerat ska tas bort eller göras obrukbara så snart som möjligt efter det att ingripandet har genomförts. Det beror på ingripandets art när det ska anses ha genomförts.

När ett ingripande har avslutats eller beslutet om ingripande har upphört att gälla är det inte tillåtet att utnyttja samma installation av tekniska hjälpmedel på nytt. Om ett nytt beslut om ingripande fattas, och det beslutet inte har fattats innan det tidigare ingripandet har upphört, måste ny installation av utrustning, programvaror eller hårdvaror göras. Ett beslut om blockering som ersätts av ett nytt beslut om samma åtgärd, innan det första beslutet har upphört, kräver dock ingen ny installation av programvara.

Skyldighet att medverka

20 §

I paragrafen regleras medverkansskyldighet för vissa privaträttsliga aktörer. Paragrafen har behandlats i avsnitt 18.4.

I *första stycket* slås fast att den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation är skyldig att, på begäran av den ingripande myndigheten, medverka vid ett ingripande i cybermiljö. Skyldigheten gäller för aktörer som tillhandahåller allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster, t.ex. mobiltelefonoperatörer.

En begäran om medverkan av den enskilde operatören ska vara proportionerlig (7 §) och endast de tekniska hjälpmedel som behövs för åtgärden får användas (17 §).

Frågan om medverkan ska väckas av den ingripande myndigheten när den har konstaterat att operatörens medverkan i något avseende behövs för att kunna genomföra ingripandet.

Den medverkande operatören ska bistå enligt myndighetens begäran. Vad en medverkan kan omfatta regleras i förordning. Vilka specifika uppgifter som en operatör ska bistå med beror på hur myndigheten formulerar sin begäran. Det kan t.ex. gälla information som gör det möjligt att närmare identifiera det informationssystem som är målet för ingripandet, upplysningar om vilka förbindelser som används av informationssystemet i fråga eller att få annan nödvändig information för att kunna begränsa ingripandet.

Av *andra stycke*t framgår att den operatör som medverkar enligt paragrafen har rätt till ersättning från myndigheten för de kostnader som uppstår vid sådan medverkan. De kostnader som avses är främst nedlagd tid hos operatören. Kostnader som inte är hänförliga till tidsåtgång kan också uppstå. Det är direkta kostnader, som nerlagd tid och upplåtande av utrymme, som kan ersättas enligt paragrafen. Kostnader som kan ha uppstått vid medverkan omfattas av paragrafen, även om ingripandet inte kan genomföras. Däremot ersätts inte kostnader som uppstår hos operatören för att generellt anpassa sina system för att möjliggöra medverkan.

Underrättelse till enskild

21 §

I paragrafen föreskrivs en skyldighet att i vissa fall underrätta en enskild om ett ingripande i cybermiljö. Paragrafen har behandlats i avsnitt 19.1.1 och 19.1.2.

Ingripanden i cybermiljö påverkar enskilda i varierande utsträckning. Underrättelseskyldigheten omfattar enligt *första stycket* endast ingripanden i form av radering och mer långvarig blockering av uppgifter. Vid radering ska underrättelse alltid lämnas, oavsett om raderingen avsett enstaka uppgifter eller samtliga uppgifter i ett informationssystem. En blockering ska ha varat längre än en månad för att underrättelseskyldighet ska gälla. Underrättelsen ska riktas till den eller de som äger eller använder det informationssystem som uppgifterna i fråga ger tillgång till eller som behandlar uppgifterna. Det kan vara både fysiska och juridiska personer.

En grundläggande förutsättning för att underrättelseskyldigheten ska gälla är att den enskilde inte har fått kännedom om ingripandet på annat sätt. Om t.ex. Polismyndigheten ingriper mot en

webbaserad marknadsplats för försäljning av droger genom att blockera tillgången till den och genom ett meddelande till dem som besöker marknadsplatsen informerar om att den har gjorts oåtkomlig vid ett polisingripande, behöver alltså ingen enskild underrättas om blockeringen. Detsamma gäller om personer har kallats till polisen för att förhöras t.ex. om sina sökningar på internet på platser som enbart förmedlar kriminella tjänster eller som informerar om hur bomber tillverkas eller rekryterar till terroristorganisationer. Den information som lämnas i brottsutredningen innebär normalt att någon underrättelse enligt denna paragraf inte behöver lämnas.

Vidare gäller undantag från underrättelseskyldigheten om det gäller sekretess enligt 18 kap. 9 § offentlighets- och sekretesslagen. Sekretessen i den bestämmelsen skyddar bl.a. kod, chiffer och liknande. Sekretessen gäller om det kan antas att syftet med metoden motverkas om uppgiften röjs. De tekniska metoder som de brottsbekämpande myndigheterna använder för att bereda sig tillgång till informationssystem och de hjälpmedel som myndigheterna utvecklar för att kunna tillämpa lagen kan i vissa fall skyddas av den sekretessen. Om så är fallet behöver någon underrättelse inte lämnas. Undantag gäller också för det fallet att åklagare ska underrätta enligt 14 § andra stycket.

Eftersom underrättelsen ska lämnas först när det lämpligen kan göras, innebär det att om sekretess till skydd för den brottsutredande verksamheten gäller gentemot den enskilde och det skulle skada utredningen att underrätta om ingripandet, får den ingripande myndigheten också dröja med underrättelsen. Det kan t.ex. aktualiseras vid ett samordnat tillslag mot misstänkta pedofiler i flera länder.

En annan förutsättning för att någon ska underrättas är givetvis att personen i fråga är känd. Cybermiljön utnyttjas i stor utsträckning av personer som inte vill förknippas med sina förehavanden. Om det inte är känt vem som ska underrättas om åtgärden, och det inte heller finns anledning att anta att han eller hon genom rimliga åtgärder kan identifieras, får underrättelse underlåtas. Det innebär att underrättelse får underlåtas i de fall där det inte är praktiskt möjligt att underrätta någon om den vidtagna åtgärden. Även i situationer där det finns anledning att anta att den enskilde åtminstone teoretiskt skulle kunna identifieras kan underrättelse underlåtas i vissa fall. Det kan vara att identifiering skulle kräva orimliga resurser eller

ta alltför lång tid. Att försöka identifiera en person som från utlandet agerar för främmande makts räkning torde i de flesta fall vara utsiktslöst. Detsamma gäller i de flesta fall personer som använder sig av sådana meddelandetjänster som brukar utnyttjas för att dölja användarens identitet och använder ett alias.

En underrättelse ska lämnas så snart det lämpligen kan göras. Det innebär att underrättelsen ska lämnas så snart syftet med raderingen eller blockeringen inte längre äventyras och det inte heller i övrigt finns något hinder mot det. Underrättelsen bör vara skriftlig för att ge den enskilde ett fullgott underlag för att eventuellt ansöka om skadestånd från staten för radering eller blockering som han eller hon anser ha varit olaglig. De närmare kraven regleras i förordning.

Enligt *andra stycket* ansvarar den myndighet som har fattat beslut om ingripanden eller, i fråga om åklagares beslut om radering, har ansökt om åtgärden för underrättelsen. Det gäller dock inte i de fall där åklagaren enligt 14 § andra stycket är skyldig att underrätta den berörde.

När ett beslut ska upphävas

22 §

I paragrafen anges när beslut enligt lagen ska upphävas. Paragrafen har behandlats i avsnitt 18.5.

Enligt paragrafen ska ett beslut om ingripande upphävas om det inte längre finns skäl för beslutet. Så kan vara fallet om ingripandet har genomförts innan tiden för det har löpt ut, eftersom ändamålet med ingripandet kan ha uppnåtts. Det finns då inte längre något behov av ingripande.

Om det under den tid som ingripandet får genomföras kommer fram att det av andra skäl inte finns något behov av ingripandet, t.ex. om förutsättningarna för beslutet har fallit bort, bör beslutet också upphävas. Det kan t.ex. visa sig att det misstänkta brottet redan har hunnit fullbordas eller att den brottsliga verksamheten har upphört. Upphävande kan även aktualiseras om den brottsliga verksamheten visade sig vara av mindre allvarlig art, vilket kan innebära att grunden för beslutet har fallit bort. Det kan även visa sig att informationssystemet som åtgärden riktar sig mot inte längre är åtkomligt eller att det

har uppstått oförutsedda tekniska hinder mot att genomföra ingripandet.

Ett beslut om ingripande ska också upphävas om det under genomförandet visar sig att beslutet var fattat på felaktiga grunder. Det kan vara fallet om det visar sig att ett ingripande avsåg ett informationssystem som tillhörde eller användes av någon annan än vad som förutsattes när beslutet om ingripande fattades.

Ett beslut kan upphävas helt eller till viss del. Det sistnämnda kan behövas t.ex. därför att en viss åtgärd inte aktualiseras.

Ett beslut ska också upphävas om det efter det att beslutet fattades kommer fram att beslutet avser ett informationssystem eller uppgifter i ett informationssystem som omfattas av förbud enligt 8 §, eftersom ingripande då inte är tillåtet. Om beslutet avser även andra informationssystem eller uppgifter som inte omfattas av förbud får ingripandet i övriga delar fortsätta.

Polismyndigheten, Säkerhetspolisen eller Tullverket ska upphäva beslut som har fattats med stöd av bestämmelserna i 11–13 §§, om inte åklagaren enligt 14 § redan har upphävt beslutet därför att det saknas grund för det.

Även om de flesta ingripanden är av kortvarig karaktär, bör den ingripande myndigheten kontinuerligt pröva om det fortsatt finns behov av ingripande när genomförandet dröjer eller pågår under en längre tid.

Dokumentation

23 §

Paragrafen, som reglerar kravet på dokumentation av såväl beslut som andra åtgärder vid ingripanden i cybermiljö, har behandlats i avsnitt 19.2.

Exempel på uppgifter som bör dokumenteras – utöver innehållet i beslutet – är vem som har fattat beslutet, när det fattades och om det har ändrats eller upphävts. Även vilka uppgifter som ingripandet avsåg, om uppgifter har förstörts till följd av att de omfattas av förbud enligt 8 § och resultatet av genomförandet bör dokumenteras. Vidare bör tidpunkten för genomförandet dokumenteras, likaså om det har funnits samtycke från innehavaren av en plats som har an-

vänts för genomförandet. Detsamma gäller uppgifter som är av betydelse för anknytningen till Sverige och svenska intressen.

Skyldigheten att dokumentera gäller både för den som fattar beslut enligt lagen, såvitt gäller uppgifter som inte framgår av beslutet, och i övrigt för den som genomför ingripandet.

Uppgifterna bör dokumenteras så att det är möjligt att följa besluten och hur ingripandena har genomförts.

Bemyndigande

24 §

Paragrafen innehåller bestämmelser om bemyndigande och har behandlats i avsnitt 18.4 och 19.1.2.

I paragrafen finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om de kompetenskrav som ska gälla för dem som ska fatta beslut enligt lagen, om de underrättelser som i vissa fall ska lämnas och om medverkan och ersättning vid genomförandet av ingripanden.

24.2 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

1 §

Paragrafen reglerar Säkerhets- och integritetsskyddsnämndens (nämndens) tillsyn. Den har behandlats i avsnitt 19.3.2.

Första och *andra styckena* är oförändrade.

I *tredje stycket* utökas nämndens skyldighet att utöva tillsyn på det sättet att lagen (2027:000) om polisiära ingripanden i cybermiljö läggs till.

Det *fjärde stycket* är oförändrat.

24.3 Förslaget till lag om ändring i lagen (2022:482) om elektronisk kommunikation

9 kap.

4 §

I paragrafen anges i fem punkter vissa undantag från de begränsningar som annars gäller enligt 1–3 §§ i fråga om behandling av trafikuppgifter. Paragrafen har behandlats i avsnitt 18.4.

Punkterna 1 och *2* är oförändrade.

Punkterna 3 och *5* ändras endast redaktionellt.

I *punkten 4*, som är ny, görs undantag även för elektroniska meddelanden som omfattas av ett beslut om ingripande enligt lagen (2027:000) om polisiära ingripanden i cybermiljö.

21 §

Paragrafen reglerar i fyra punkter i vilken utsträckning lagrade uppgifter får lämnas ut. Den har behandlats i avsnitt 18.4.

Punkten 1 är oförändrad.

Punkterna 2 och 3 ändras endast redaktionellt.

I *punkten 4*, som är ny, läggs lagen (2027:000) om polisiära ingripanden i cybermiljö till.

32 §

Paragrafen reglerar viss tystnadsplikt. Paragrafen har behandlats i avsnitt 20.4.2.

I åtta punkter föreskrivs att tystnadsplikt gäller för bl.a. angelägenheter som rör hemliga tvångsmedel och vissa andra brottsbekämpande åtgärder.

Punkterna 1–5 är oförändrade.

Punkterna 6 och *7* ändras endast redaktionellt.

I *punkten 8* läggs en begäran enligt 20 § lagen (2027:000) om polisiära ingripanden i cybermiljö till.

24.4 Förslaget till lag om ändring i tullbefogenhetslagen (2024:710)

7 kap.

5 a §

Paragrafen, som är ny, har behandlats i avsnitt 20.5. I paragrafen påminns om att det i lagen (2027:000) om polisiära ingripanden i cybermiljö finns bestämmelser om Tullverkets rätt att ingripa i cybermiljö.

Särskilt yttrande av experterna Ida Olsson och Andreas Persson

Inledning

Vi delar utredningens uppfattning att de brottsbekämpande myndigheterna har ett angeläget behov av att kunna ingripa mot vissa brott i cybermiljö och att den befintliga lagstiftningen är otillräcklig för att tillgodose detta behov. Liksom utredningen anser vi att det behövs ny lagstiftning som ger myndigheterna verktyg för att ingripa mot sådana brott.

Vi anser dock att den föreslagna lagen inte är tillräckligt avgränsad och att den inte omgärdas av tillräckliga rättssäkerhetsgarantier. Den bedömningen gör vi mot bakgrund av att ingripandena i cybermiljö har stora likheter med hemlig dataavläsning och kan innebära stora integritetsintrång.

Utgångspunkter för vår bedömning

Ingripanden i cybermiljö har stora likheter med hemlig dataavläsning

Utredningen menar att ingripanden i cybermiljö skiljer sig från hemliga tvångsmedel, såsom hemlig dataavläsning, bl.a. eftersom ingripandena förväntas ske helt öppet och inte syftar till att systematiskt och under längre tid samla in information för att utreda brott eller berika underrättelseverksamhet. Vi delar inte utredningens uppfattning om hur betydande skillnaderna är.

Vid ingripanden enligt lagen ska de brottsbekämpande myndigheterna få bereda sig tillgång till informationssystem genom att bryta systemskydd eller utnyttja tekniska sårbarheter (17 §). Detta kan

jämföras med det sätt som myndigheterna tar sig in i informationssystem vid genomförande av hemlig dataavläsning (jfr 1 och 22 §§ lagen [2020:62] om hemlig dataavläsning).

Syftet med den föreslagna regleringen är visserligen – till skillnad från vad som gäller för hemliga tvångsmedel – inte att hämta in information för att kunna utreda brott eller berika underrättelseverksamhet. Det anges också i betänkandet att lagen inte medger att myndigheterna hämtar in uppgifter genom att t.ex. kopiera dem eller på annat sätt föra över dem till ett eget informationssystem på det sätt som är fallet vid hemlig dataavläsning. I författningskommentaren anges emellertid att sådan inhämtning får göras, om det är ett absolut nödvändigt steg för att kunna genomföra någon del av ingripandet. Någon begränsning i fråga om inhämtning av uppgifter finns dock inte i lagtexten. Inte heller föreskrivs någon begränsning gällande hur information som myndigheterna får tillgång till genom ett ingripande får användas i andra syften. Vi noterar också att det i betänkandet anges flera exempel på hur information från ett ingripande ska kunna användas i underrättelseverksamhet och i förundersökningar.

Vi anser vidare att de föreslagna ingripandenas varaktighet inte har någon avgörande betydelse för frågan om de skiljer sig från hemliga tvångsmedel. Det är inte alltid som hemliga tvångsmedel används systematiskt och under längre tid. Det gäller även hemlig dataavläsning. Ingripandenas kortvariga karaktär återspeglas inte heller tydligt i den föreslagna lagtexten.

Enligt vår mening är det slutligen inte helt rättvisande att påstå att ingripanden enligt den nya lagen normalt förväntas göras helt öppet. Den del av ingripandet som innebär att myndigheten bereder sig tillgång till ett informationssystem sker ofta utan att användaren vet om det. Detta får till följd att användaren oftast inte upptäcker att en åtgärd vidtagits i de fall då myndigheten därefter bedömer att det saknas förutsättningar att t.ex. blockera eller radera uppgifter. Vidare uppställs det inte något krav på att den brottsbekämpande myndigheten ska lämna information i systemet eller på motsvarande sätt upplysa om att myndigheten t.ex. ändrat, blockerat eller raderat uppgifter. Även om det kan hända att den enskilde, vars informationssystem blir föremål för ett ingripande, uppmärksammar att uppgifter t.ex. blockerats är det som utredningen framhåller inte självklart att den enskilde förstår vem som har utfört blockeringen. När

det slutligen gäller ingripanden enligt 4 § måste sådana åtgärder i regel ske helt dolt för att vara verksamma.

Sammanfattningsvis anser vi att ingripanden i cybermiljö har påtagliga likheter med hemlig dataavläsning och det integritetsintrång som detta tvångsmedel kan innebära.

Ingripanden enligt lagen kan innebära stora integritetsintrång

Oavsett jämförelsen med befintliga tvångsmedel kan det konstateras att ingripandena kan innebära stora integritetsintrång. Redan det moment som ett ingripande i regel inleds med, dvs. att bereda sig tillgång till uppgifter i ett informationssystem, kan innebära ett allvarligt intrång. Det gäller oavsett vad syftet med ingripandet är. Hur mycket information eller vilken typ av information som myndigheterna kan komma att ta del av vid ett ingripande är vidare svårt att förutse. Även de åtgärder som innebär att myndigheterna ändrar, blockerar eller raderar uppgifter i informationssystemet kan innebära allvarliga intrång i den personliga integriteten.

Vi delar visserligen utredningens uppfattning att integritetsintrånget kan variera beroende på omständigheterna i det enskilda fallet. Vi anser dock att lagstiftningen måste utformas med beaktande av de fall där riskerna för integritetsintrång är som störst.

Synpunkter på lagens avgränsning och utformning

Lagen är inte tillräckligt avgränsad

Att ingripanden enligt lagen kan innebära stora integritetsintrång innebär enligt vår mening att det bör ställas höga krav på hur lagen avgränsas.

Enligt förslaget ska lagen avgränsas genom att åtgärderna endast får avse brott, eller brottslig verksamhet som innefattar brott, för vilket det är föreskrivet fängelse i ett år eller mer. Vi menar att gränsdragningen medför att lagens tillämpningsområde blir för brett och omfattar fler brott än de som myndigheterna främst har redovisat behov av att använda ingripandena mot. Som en jämförelse kan också nämnas att det enligt huvudregeln krävs ett minimistraff på sex månaders fängelse för att kunna använda hemlig övervakning av elektro-

nisk kommunikation, som är det hemliga tvångsmedel som generellt anses vara minst ingripande. Det kan även jämföras med den avgränsning som gjorts i den föreslagna lagen om avlägsnande av rekryteringsinnehåll online. Avgränsningen till brott för vilket det är föreskrivet fängelse i ett år eller mer saknar vidare motsvarighet i den internationella utblick som utredningen gjort. Det vida tillämpningsområdet kan enligt vår mening inte anses uppvägas av att ingripandena, på grund av de resurser de tar i anspråk, i praktiken inledningsvis förväntas avse endast vissa kategorier av brott.

Lagens tillämpningsområde avgränsas också genom att ingripanden endast får avse brott, eller brottslig verksamhet som innefattar brott, som begås eller kommer att begås i cybermiljö. Vi anser att den föreslagna innebörden av att ett brott begås i cybermiljö inte är tillräckligt preciserad och befarar att det kommer att leda till att lagen tillämpas i flera fall än vad som är avsett.

Det uppställs vidare, för ingripanden enligt 3 och 5 §§, inte något krav på att de brottsbekämpande myndigheterna med viss styrka ska misstänka att ett visst informationssystem används för brott eller bedöma att det finns risk för att ett sådant kommer att användas vid brottslig verksamhet. Att ett ingripande ska vara av särskild eller synnerlig vikt för att i cybermiljö förhindra eller avbryta brott, eller störa eller avbryta brottslig verksamhet, kan enligt vår mening inte kompensera för avsaknaden av misstanke- respektive riskrekvisit.

Sammantaget anser vi att lagen inte är tillräckligt avgränsad i förhållande till de risker för integritetsintrång som den medför.

Rättssäkerhetsgarantierna är inte tillräckliga

Att ingripanden i cybermiljö kan innebära stora integritetsintrång ställer också höga krav på rättssäkerhetsgarantier. Vi anser att de rättssäkerhetsgarantier som föreslås i lagen inte är tillräckliga.

Till att börja med innebär den förslagna ordningen att domstol varken beslutar om ingripande eller har möjlighet att pröva beslut om ingripande i efterhand. Vi noterar också att beslutsordningen framstår som avvikande i den internationella utblick som utredningen gjort. Därutöver saknas allmän reglering om granskning, bevaring och förstöring av uppgifter som de brottsbekämpande myndigheterna i vissa fall kan komma att hämta in när de bereder sig tillgång till ett

informationssystem. Som vi konstaterat är det inte heller reglerat hur information som myndigheterna får tillgång till under ett ingripande får användas i andra syften. Trots att ingripanden i cybermiljö inte alltid kan anses äga rum öppet föreslås det vidare inte någon generell skyldighet att i efterhand underrätta den enskilde som varit föremål för ett ingripande. Även om den enskilde blir underrättad – eller på annat sätt förstår att ett ingripande genomförts – finns det dessutom inte någon generell lagreglerad möjlighet för honom eller henne att invända mot ett beslut om ingripande och verka för att t.ex. en blockering ska hävas.

Sammantaget anser vi att det krävs ytterligare rättssäkerhetsgarantier för att väga upp det integritetsintrång som ingripandena kan innebära.

Avslutande synpunkter

Vi invänder inte mot att myndigheterna, under vissa omständigheter, ska ges möjlighet att t.ex. bereda sig tillgång till ett informationssystem och ändra, blockera eller radera uppgifter i detta. Mot bakgrund av att verktygen kan innebära stora intrång i enskildas personliga integritet och att det är svårt att överblicka hur den nya lagen kan komma att tillämpas anser vi emellertid att regleringen bör utformas med försiktighet. Eftersom lagen föreslås vara tidsbegränsad finns möjlighet att justera och utvidga regleringen när den tillämpats en tid och ingripandenas praktiska tillämpning och effekter utvärderats.

Särskilt yttrande av experten Bengt Ivarsson

Jag ansluter mig till det yttrande som avgivits av experterna Ida Olsson och Andreas Persson. Utöver detta vill jag tillägga följande.

De aktörer som kan bli föremål för åtgärder enligt lagen är av vitt skilda typer. Det kan röra sig om enskilda personer där integritetsintrånget blir högst påtagligt och därmed leder till att rättssäkerhetsgarantierna blir extra viktiga. I andra fall kan det avse främmande makt med stora resurser och obefintligt integritetsintrång och betydligt lägre behov av rättssäkerhetsgarantier. Det sagda innebär att det är svårt att hitta en rimlig och enhetlig nivå i dessa frågor.

Kommittédirektiv 2025:12

Hemliga och preventiva tvångsmedel – en effektiv och tydlig reglering

Beslut vid regeringssammanträde den 20 februari 2025.

Sammanfattning

En särskild utredare ges i uppdrag att göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel i syfte att åstadkomma en mer effektiv och tydlig reglering och att förbättra möjligheterna att använda tvångsmedlen i brottsbekämpningens olika faser.

- Utredaren ska bl.a.
- utvärdera tillämpningen av de utökade möjligheterna att använda hemliga och preventiva tvångsmedel och kartlägga den nytta som dessa inneburit för brottsbekämpningen i stort,
- ta ställning till om de under viss tid utökade möjligheterna att använda preventiva tvångsmedel, vilka bl.a. innebär att hemlig avlyssning och övervakning kan användas för att förhindra särskilt allvarlig brottslighet inom kriminella nätverk, ska fortsätta att gälla utan tidsbegränsning,
- göra en analys av den samlade regleringens konsekvenser för den personliga integriteten,
- analysera behovet och nyttan av samt föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö, eller vidta andra jämförbara åtgärder i sådan miljö, i syfte

att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot sådan brottslighet, och

- lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder.
- Uppdraget ska redovisas senast den 29 maj 2026.

Regleringen om hemliga och preventiva tvångsmedel

För att lyckas i sitt uppdrag att bekämpa den allvarliga brottsligheten behöver de brottsbekämpande myndigheterna ändamålsenliga och verkningsfulla verktyg. Hemliga och preventiva tvångsmedel är ofta helt avgörande för att förebygga, utreda och lagföra allvarlig brottslighet. Särskilt viktiga är hemliga och preventiva tvångsmedel i kampen mot den organiserade brottsligheten. För att hemliga och preventiva tvångsmedel ska fortsätta att vara effektiva verktyg för de brottsbekämpande myndigheterna krävs det emellertid att regleringen både är ändamålsenlig och lätt att tillämpa.

Hemliga tvångsmedel får användas i brottsbekämpningens olika faser

Hemliga tvångsmedel kan idag användas i olika skeden av det brottsbekämpande arbetet, både för att förebygga, förhindra eller upptäcka allvarlig brottslig verksamhet i underrättelseverksamhet (s.k. preventiva tvångsmedel) och för att utreda brott i en förundersökning. Sedan den 1 juli 2024 är det även möjligt att använda vissa hemliga tvångsmedel för att lokalisera personer som håller sig undan eller har avvikit från ett beslut om anhållande eller häktning eller från verkställighet av ett straff.

Med hemliga tvångsmedel avses traditionellt sett de tvångsmedel som kategoriseras som hemliga i 27 kap. rättegångsbalken, dvs. hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och postkontroll. Till de hemliga tvångsmedlen räknas också hemlig dataavläsning som regleras i lagen (2020:62) om hemlig dataavläsning. De hemliga tvångsmedlen intar en särställning bland de straffprocessuella tvångsmedlen eftersom den som tvångsmedlet riktas mot är ovetande om tvångsmedelsanvändningen. Det är inte bara verkställigheten som

äger rum i hemlighet, utan även prövningen av om tvångsmedlen får användas. Att tvångsmedelsanvändningen sker i hemlighet är nämligen en förutsättning för att tvångsmedlen ska få avsedd effekt. Den som har varit föremål för ett hemligt tvångsmedel ska som huvudregel underrättas om det i efterhand. Det finns dock undantag från den underrättelseskyldigheten.

Förundersökningsverksamheten regleras utförligt i rättegångsbalken och i förundersökningskungörelsen (1947:948). Av 23 kap. 1 § rättegångsbalken följer att en förundersökning ska inledas så snart det finns anledning att anta att ett brott som hör under allmänt åtal har begåtts. Det krävs alltså att det finns en misstanke om ett visst konkret brott för att en förundersökning ska kunna inledas. Enbart lösa antaganden om att en person är inblandad i viss typ av brottslighet anses inte utgöra en tillräcklig grund för att inleda en förundersökning. Ett beslut att inleda en förundersökning fattas enligt 23 kap. 3 § rättegångsbalken av Polismyndigheten, Säkerhetspolisen eller åklagaren. En förundersökning kan också inledas av andra myndigheter (se t.ex. 3 kap. 3 § kustbevakningslagen [2019:32] och 8 kap. 3 § tullbefogenhetslagen [2024:710]). Möjligheterna att använda hemliga tvångsmedel i en förundersökning regleras i 27 kap. rättegångsbalken och lagen (2020:62) om hemlig dataavläsning.

Underrättelseverksamhet, som bl.a. bedrivs av Polismyndigheten, Säkerhetspolisen och Tullverket, innebär insamling, bearbetning och analys av information som senare kan ha betydelse för att förhindra eller för att utreda brott. Det handlar alltså om informationsinsamling redan innan det finns en mer konkretiserad misstanke om ett visst brott. Den tvångsmedelsanvändning som tillåts i underrättelseverksamheten regleras i flera lagar, bl.a. i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) och lagen om hemlig dataavläsning. De tvångsmedel som sedan den 1 september 2024 får användas i preventivt syfte är dels de tvångsmedel som traditionellt sett är att betrakta som hemliga tvångsmedel, dels husrannsakan, undersökning på annat ställe och genomsökning på distans (1–1 c §§ preventivlagen). Till skillnad från vad som gäller när en husrannsakan, en undersökning på annat ställe och en genomsökning på distans används i en förundersökning får tvångsmedlen inom ramen för under-

rättelseverksamheten verkställas i hemlighet. Därutöver finns det regler om tvångsmedel som får användas för att upptäcka eller förebygga brott i vissa andra lagar, exempelvis i polislagen (1984:387), lagen (2022:700) om särskild kontroll av vissa utlänningar, lagen (2023:474) om polisiära befogenheter i gränsnära områden och tullbefogenhetslagen.

Vissa hemliga tvångsmedel, nämligen hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter, får sedan den 1 juli 2024 även användas i verkställighetsstadiet. Tvångsmedlen får då användas för att lokalisera personer som håller sig undan eller har avvikit från verkställighet av en utdömd påföljd. Reglerna finns i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

Flera kriminella individer uppehåller sig i andra länder och bedriver därifrån organiserad brottslig verksamhet riktad mot Sverige. Att få assistans med utredningsåtgärder utomlands har därför blivit en allt viktigare del i arbetet med att bekämpa organiserad brottslighet. Författningsstöd för att använda hemliga tvångsmedel i det internationella straffrättsliga samarbetet finns bl.a. i lagen (2017:1000) om en europeisk utredningsorder och lagen (2000:562) om internationell rättslig hjälp i brottmål. Regler om hemliga tvångsmedel i fråga om utlänningsärenden med s.k. kvalificerade säkerhetsaspekter, dvs. ärenden där utlänningen har utvisats eftersom denne kan antas komma att begå eller på annat sätt medverka till ett brott enligt terroristbrottslagen (2022:666) eller kan utgöra ett allvarligt hot mot Sveriges säkerhet, finns i lagen (2022:700) om särskild kontroll av vissa utlänningar.

Enskildas grundläggande fri- och rättigheter

Användning av hemliga och preventiva tvångsmedel innebär en inskränkning av enskildas grundläggande fri- och rättigheter, bl.a. i form av en risk för ingrepp i enskildas personliga integritet. Föreskrifter om skydd för grundläggande fri- och rättigheter finns bl.a. i regeringsformen, den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och Europeiska unionens stadga om de grundläggan-

de rättigheterna (EU:s rättighetsstadga). Därutöver innehåller Förenta nationernas konvention om barnets rättigheter (barnkonventionen) bestämmelser om barns rättigheter. Sverige har även förbundit sig att följa flera andra internationella åtaganden om mänskliga rättigheter, bl.a. Internationella konventionen om medborgerliga och politiska rättigheter. Dessa grundläggande fri- och rättigheter får bara begränsas på särskilt angivna sätt. När det gäller t.ex. skyddet i 2 kap. 6 § regeringsformen mot olika typer av integritetsintrång måste begränsningen ske genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som motiverat dem och inte heller utgöra ett hot mot den fria åsiktsbildningen. Vid införandet av utökade möjligheter att använda hemliga och preventiva tvångsmedel är det alltså nödvändigt att, utifrån det specifika ändamål som ska uppnås med åtgärden, kartlägga behovet och den förväntade nyttan av åtgärden och se till att regleringen utformas på ett sådant sätt att såväl den enskilda åtgärden som den samlade inverkan av tvångsmedel innebär en proportionerlig inskränkning av grundläggande fri- och rättigheter. Förslagen måste också vara förenliga med högt ställda krav på rättssäkerhet.

Det ska även framhållas att staten enligt artikel 8 i Europakonventionen har en positiv förpliktelse att se till att enskilda tillförsäkras skydd för bl.a. sitt privat- och familjeliv gentemot andra enskilda. Det innebär t.ex. att staten i vissa fall kan vara skyldig att införa straffrättslig reglering för att skydda enskilda mot ingrepp i deras rättigheter från andra enskilda. Det innebär också att staten för sådana fall behöver säkerställa att brott kan utredas effektivt. Den analys av proportionaliteten och effekter för integriteten som ska göras behöver därför innefatta en avvägning mellan å ena sidan det integritetsintrång som hemliga eller preventiva tvångsmedel innebär för den enskilde och å andra sidan det integritetsintrång som brottsligheten innebär för brottsoffer.

Uppdraget att göra en rättslig och systematisk översyn av regleringen

I takt med att samhället, tekniken och brottsligheten har utvecklats har också regleringen om hemliga och preventiva tvångsmedel ändrats och byggts ut. Regleringen finns i dag i flera lagar med delvis olika rekvisit, kvalifikationskrav och ändamålsbestämmelser. Regelverket är komplext och bestämmelserna kan vara svåra att tillgodogöra sig. Även om reglerna i tidigare lagstiftningsärenden har bedömts uppfylla de minimigarantier som utvecklats i Europadomstolens praxis (jfr t.ex. Europadomstolens dom den 4 december 2015 i målet Roman Zakharov mot Ryssland, nr 47143/06, punkt 231) är det av stor vikt att säkerställa att regleringen är överblickbar och lätt att tillämpa. Reglerna om hemliga och preventiva tvångsmedel bör därför ses över med målsättningen att skapa en så tydlig och pedagogisk reglering som möjligt. En sådan översyn ska omfatta såväl regleringens systematik som de rättsliga förutsättningarna för att använda hemliga och preventiva tvångsmedel.

När det gäller regleringens systematik kan det t.ex. övervägas om det även fortsatt är lämpligt att reglerna om hemliga och preventiva tvångsmedel är spridda i flera lagar. Ett flertal aktörer som tillämpar reglerna vittnar om att regleringen är svåröverskådlig. En möjlig lösning skulle därför kunna vara att samla reglerna om hemliga och preventiva tvångsmedel i en lag. En sammanhållen reglering skulle också kunna medföra att behovet av att ha bestämmelser med liknande innehåll i flera olika lagar minskar. Det kan även finnas fördelar med att reglerna om hemliga och preventiva tvångsmedel fortsatt är uppdelade i olika lagar, t.ex. med hänsyn till bestämmelsernas syfte och tillämpningsområde. En annan lösning skulle därför kunna vara att genomföra en omstrukturering av bestämmelserna inom ramen för de befintliga lagarna eller inom ramen för flera nya lagar.

Utöver att systematiken i regleringen om hemliga och preventiva tvångsmedel behöver ses över finns det ett behov av att göra en översyn av de enskilda paragraferna och deras inbördes systematik. En del paragrafer är mycket långa medan andra paragrafer innehåller hänvisningar, antingen till andra paragrafer eller till andra lagar, vilket gör det svårt för läsaren att ta till sig texten. Även begreppsanvändningen i de olika lagarna är delvis omodern och kan dessutom variera mellan lagarna. Ett exempel i det avseendet är bestämmel-

serna om granskning av material från hemliga tvångsmedel och förstöring av sådant material som inte följt teknikutvecklingen. Därutöver behöver ändamålsbestämmelserna i de olika lagarna ses över.

När det gäller de rättsliga förutsättningarna för att använda hemliga och preventiva tvångsmedel måste positionerna flyttas fram ytterligare. Det måste säkerställas att de brottsbekämpande myndigheterna har tillgång till verkningsfulla och moderna verktyg i brottsbekämpningens olika faser. De kriminella aktörerna är ytterst säkerhetsmedvetna och de brottsbekämpande myndigheterna måste ges förutsättningar att ligga steget före dem. Det är också angeläget att se till att de svenska myndigheterna har tillgång till verktyg som motsvarar de som finns i andra jämförbara länder. Myndigheterna verkar på en alltmer internationell arena där rättsligt samarbete länder emellan blir allt viktigare. En internationell utblick och kartläggning av hur motsvarande reglering ser ut i andra jämförbara länder bör därför göras. Dessutom finns det anledning att överväga om det går att uppnå en större flexibilitet i regleringen om hemliga och preventiva tvångsmedel så att tvångsmedlen kan användas när det framstår som motiverat.

Några exempel på hur reglerna kan behöva ses över:

- En modifiering av kravet på att hemliga tvångsmedel ska avse en identifierad person
- Förbättrade möjligheter att använda hemlig avlyssning och övervakning av elektronisk kommunikation
- Förbättrade möjligheter att använda hemlig kameraövervakning och hemlig rumsavlyssning
- En effektivare tillståndsprocess och ett förändrat system för underrättelser om hemliga och preventiva tvångsmedel.

Nedan följer en mer utförlig beskrivning av de nämnda exemplen.

En modifiering av kravet på att hemliga tvångsmedel ska avse en identifierad person

Regleringen om hemliga och preventiva tvångsmedel är utformad på så sätt att det krävs att åtgärden avser en identifierad person. I en förundersökning måste åtgärden som huvudregel avse en skäligen

misstänkt person, medan det i underrättelseskedet krävs att åtgärden avser en person som kan komma att utöva viss brottslig verksamhet eller, när brottsligheten begås inom en organisation eller grupp, en person som tillhör organisationen eller gruppen och främjar denna brottslighet. Det finns goda skäl för att regleringen har utformats på det sättet, inte minst för att undvika en mer generell övervakning. Kravet på att åtgärden ska avse en identifierad person kan emellertid, med hänsyn till hur brottsligheten har utvecklats över tid och de tekniska framsteg som gjorts, innebära problem vid tillämpningen. Exempel på det är när allvarliga brott begås av flera personer inom ramen för ett kriminellt nätverk eller av en statlig aktör och det av olika skäl inte går att klargöra exakt vem som ligger bakom ett visst agerande. Sådana svårigheter uppstår i synnerhet när brott begås i cybermiljön eller med hjälp av digitala verktyg. Det finns därför skäl att överväga om kravet på att åtgärden måste avse en identifierad person kan modifieras så att hemliga och preventiva tvångsmedel kan användas mer effektivt i de situationer där det framstår som motiverat. Det kan t.ex. handla om att använda sådana tvångsmedel mot en statlig aktör eller mot en kriminell sammanslutning.

Förbättrade möjligheter att använda hemlig avlyssning och övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation i form av en s.k. basstationstömning, dvs. inhämtning av uppgifter om vilka elektroniska kommunikationsutrustningar som funnits inom ett visst geografiskt område, kan bl.a. användas för att utreda vem som skäligen kan misstänkas för ett visst brott (se t.ex. 27 kap. 19 och 19 b §§ rättegångsbalken). Om polisen under fysisk spaning kan se att den misstänkte flera gånger på olika platser använder en annan telefon än den polisen känner till skulle en basstationstömning på de platser och tidpunkter där den okända telefonen använts kunna medföra att telefonen kan identifieras och avlyssnas eller övervakas. De kriminella aktörerna är ytterst säkerhetsmedvetna och byter regelbundet telefoner för att undvika avlyssning eller övervakning, varför det kan finnas behov av en utökad möjlighet till basstationstömning, t.ex. för att söka fram nya telefonnummer till en redan skäligen misstänkt person.

Hemlig avlyssning och övervakning av elektronisk kommunikation kan i vissa fall riktas mot t.ex. en teleadress eller kommunikationsutrustning som det finns synnerlig anledning att anta att en brottsmisstänkt person har kontaktat eller kommer att kontakta. Utifrån rådande rättspraxis är det oklart om avlyssning eller övervakning får riktas mot en sådan kontaktperson som inte har fyllt 15 år. Med hänsyn till dagens brottsutveckling där mycket allvarliga brott begås av barn under 15 år finns det ett stort behov av att kunna rikta avlyssning eller övervakning mot kontaktpersoner som inte har fyllt 15 år. Det kan därför finnas skäl att titta närmare på frågan och ta ställning till om det behövs regeländringar för att möjliggöra detta.

Förbättrade möjligheter att använda hemlig kameraövervakning och hemlig rumsavlyssning

Hemlig kameraövervakning och hemlig rumsavlyssning ska enligt nuvarande ordning som huvudregel riktas mot en plats där det finns anledning att anta att den misstänkte kan komma att uppehålla sig (se t.ex. 27 kap. 20 b § andra stycket rättegångsbalken). Detsamma gäller för hemlig dataavläsning som gäller kameraövervaknings- eller rumsavlyssningsuppgifter (se t.ex. 4 a § tredje stycket lagen om hemlig dataavläsning). Endast om det finns särskilda skäl får övervakningen eller avlyssningen knytas till en person i stället för en plats (se t.ex. 27 kap. 20 b § tredje stycket rättegångsbalken och 4 a § fjärde stycket lagen om hemlig dataavläsning). Det innebär att en polisman eller en tulltjänsteman med en drönare kan följa t.ex. en narkotikakurir som bär ett parti narkotika med sig. Om kuriren lämnar över narkotikan till en annan person saknas dock rättslig grund för att fortsätta övervakningen eller avlyssningen mot den nya innehavaren av narkotikan. För att övervakningen eller avlyssningen ska kunna fortgå krävs ett nytt tillstånd riktat mot den nya innehavaren. Så länge personen är oidentifierad är det inte möjligt att utverka ett sådant tillstånd. Ett sådant tillståndsbeslut måste dessutom kunna fattas minutoperativt, dvs. utan onödig tidsåtgång, vilket sällan är möjligt. En möjlighet att med hemlig kameraövervakning följa t.ex. ett parti narkotika vore ett mycket användbart verktyg i det brottsbekämpande arbetet och det bör övervägas om en sådan möjlighet bör införas.

Hemlig kameraövervakning och hemlig dataavläsning som gäller kameraövervakningsuppgifter kan riktas mot en brottsplats för att utreda vem som skäligen kan misstänkas för ett brott (se t.ex. 27 kap. 20 c § rättegångsbalken). I vissa situationer, t.ex. när ett brott begås av flera samverkande gärningsmän och endast en av gärningsmännen är identifierad, kan det emellertid finnas ett behov av att rikta sådan övervakning mot en brottsplats för att utreda vilka andra personer som skäligen kan misstänkas för brottet. Med hänsyn till hur lagtexten är formulerad är det oklart om hemlig kameraövervakning får användas i en sådan situation. Det bör därför övervägas om hemlig kameraövervakning, och hemlig dataavläsning som gäller motsvarande uppgifter, bör få användas i en sådan situation.

Vid verkställighet av hemlig kameraövervakning och hemlig dataavläsning som gäller kameraövervakningsuppgifter får inte ljud tas upp. Det kan innebära att de brottsbekämpande myndigheterna inte kan följa en dialog som förs mellan gärningsmän som t.ex. återbesöker en brottsplats. Det bör därför övervägas om även hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter bör kunna riktas mot en brottsplats för att utreda vem som skäligen kan misstänkas för ett brott.

En effektivare tillståndsprocess och ett förändrat system för underrättelser om hemliga och preventiva tvångsmedel

Ett snabbt beslutsfattande är av yttersta vikt när det gäller hemliga och preventiva tvångsmedel. Det är domstolen som, på ansökan av åklagaren, prövar om tillstånd ska beviljas. I de allra flesta fall ska domstolen utse ett offentligt ombud och hålla sammanträde i ärendet. Åklagaren kan i brådskande fall interimistiskt besluta om hemliga och preventiva tvångsmedel. Åklagarbeslutet ska i sådana fall underställas domstolen som ska pröva om åklagaren har haft skäl för åtgärden. Inom det internationella straffrättsliga samarbetet uppställs vissa krav på tillståndsprocessen t.ex. när det gäller vem som får ansöka om rättslig hjälp i fråga om hemliga tvångsmedel.

Det bör övervägas om tillståndsprocessen kan effektiviseras. Det kan handla om att ett förenklat förfarande i domstolarna kan användas i större utsträckning än i dag, t.ex. när det är fråga om förlängning av ett tillstånd. Det kan också handla om att låta särskilt kvalificerade befattningshavare inom t.ex. Polismyndigheten, Säkerhets-

polisen eller Tullverket fatta vissa mycket brådskande beslut interimistiskt. Processen bör så långt som möjligt vara enhetlig för att underlätta den praktiska hanteringen och den får inte vara allt för administrativt betungande för de brottsbekämpande myndigheterna eller för domstolarna.

Som huvudregel gäller vidare att den som har varit föremål för hemliga eller preventiva tvångsmedel ska underrättas om det. Det finns dock undantag från den regeln, t.ex. om det råder sekretess. Även inom det internationella straffrättsliga samarbetet finns vissa krav på underrättelser till enskilda vid användning av hemliga tvångsmedel. Frågan om underrättelse ska ske eller inte tar stora resurser i anspråk hos myndigheterna trots att det i realiteten är mycket få personer som faktiskt underrättas om att hemliga eller preventiva tvångsmedel använts. I de allra flesta fall underrättas i stället Säkerhets- och integritetsskyddsnämnden om tvångsmedelsanvändningen. Det kan därför finnas skäl att kartlägga hur dagens system med underrättelser fungerar i praktiken och överväga om den regleringen bör ändras, tex. på så sätt att endast Säkerhets- och integritetsskyddsnämnden ska underrättas om tvångsmedelsanvändningen.

Sammanfattning av uppdraget att göra en rättslig och systematisk översyn av regleringen

I ljuset av den senaste tidens reformer behöver regleringen om hemliga och preventiva tvångsmedel ses över i ett sammanhang med målsättningen att uppnå en så tydlig och effektiv reglering som möjligt. Möjligheterna att använda hemliga och preventiva tvångsmedel i brottsbekämpningens olika faser måste också förbättras.

Utredaren ska därför

- kartlägga och redovisa andra jämförbara länders regelverk om hemliga och preventiva tvångsmedel eller motsvarande åtgärder,
- göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel i syfte att åstadkomma en reglering som är enhetlig, tydlig och lätt att tillämpa,
- analysera hur reglerna om hemliga och preventiva tvångsmedel kan ändras för att vara än mer verkningsfulla i brottsbekämpningen, och
- lämna nödvändiga författningsförslag.

Uppdraget att utvärdera de utökade möjligheterna att använda hemliga och preventiva tvångsmedel

Under de senaste åren har flera reformer som tar sikte på att förbättra möjligheterna att använda hemliga och preventiva tvångsmedel genomförts. Reformtakten har varit hög men behovet av reformer och en starkare lagstiftning på området har också varit stort till följd av bl.a. utvecklingen när det gäller den organiserade brottsligheten. Regeringen anser att en snabbhet i förfarandet har varit absolut nödvändigt för att möta den exceptionella brottsutvecklingen i Sverige.

Möjligheterna att använda hemliga tvångsmedel i en förundersökning har utökats bl.a. på så sätt att hemliga tvångsmedel får användas för att utreda fler typer av brott, att hemliga tvångsmedel får användas för att utreda flera brott vars samlade straffvärde överstiger en viss nivå och att hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning som gäller motsvarande uppgifter får knytas till en person i stället för en plats. Samtidigt har reglerna om överskottsinformation ändrats och det har införts regler som förbättrar möjligheterna till tillsyn och insyn, t.ex. ett krav på dokumentation (propositionen Hemliga tvångsmedel – effektiva verktyg för att förebygga och förhindra allvarliga brott, prop. 2022/23:126).

Även möjligheterna att använda preventiva tvångsmedel har utökats i flera olika avseenden. I ett första skede blev det möjligt att med stöd av preventivlagen och lagen om hemlig dataavläsning använda preventiva tvångsmedel för att förhindra vissa särskilt allvarliga brott som förekommer inom kriminella nätverk (prop. 2022/23:126). I ett andra skede blev det möjligt att med stöd av inhämtningslagen och lagen om hemlig dataavläsning inhämta vissa uppgifter om elektronisk kommunikation i fråga om fler typer av brott, t.ex. grov stöld, grovt bedrägeri, grovt skattebrott och grovt bidragsbrott. Samtidigt utökades den preventiva tvångsmedelskatalogen i preventivlagen och lagen om hemlig dataavläsning. Det blev alltså möjligt att använda fler tvångsmedel och vissa verkställighetsåtgärder, t.ex. hemlig rumsavlyssning och husrannsakan, i preventivt syfte. Därtill ändrades reglerna om överskottsinformation och det infördes regler i syfte att förbättra rättssäkerheten, t.ex. utökade förbud mot avlyssning och övervakning (propositionen Preventiva tvångsmedel för att förebygga och förhindra allvarliga brott, prop.

2023/24:117). Av integritetsskäl tidsbegränsades de utökade möjligheterna att använda preventiva tvångsmedel att gälla till utgången av september 2028.

Det har vidare införts regler som innebär att vissa hemliga tvångsmedel får användas för att lokalisera personer som håller sig undan eller har avvikit från ett beslut om anhållande eller häktning eller från verkställighet av ett straff (propositionen Bättre möjligheter att verkställa frihetsberövanden, prop. 2023/24:108). I november 2024 överlämnade regeringen dessutom propositionen Hemlig dataavläsning mot allvarliga brott (prop. 2024/25:51) till riksdagen med förslag som bl.a. innebär att lagen om hemlig dataavläsning ska gälla utan tidsbegränsning. Lagändringarna föreslås träda i kraft den 1 april 2025.

Tillämpningen av de nya reglerna om hemliga och preventiva tvångsmedel behöver utvärderas. Att en utvärdering bör ske har även framhållits av både remissinstanserna och Lagrådet i flera lagstiftningsärenden om hemliga och preventiva tvångsmedel på senare tid. En sådan utvärdering bör innefatta dels en utvärdering av den nytta som regleringen har inneburit för det brottsbekämpande arbetet i stort, dels en förnyad kartläggning av de brottsbekämpande myndigheternas behov av regleringen. Därtill bör det övervägas om det finns utrymme för förbättringar av reglerna så att de blir än mer träffsäkra i tillämpningen. Samtidigt bör en utredare ta ställning till om den tidsbegränsade regleringen för vissa preventiva tvångsmedel bör gälla utan tidsbegränsning. I och med att lagstiftningstakten på det hemliga och preventiva tvångsmedelsområdet har varit hög behöver det även tas ett samlat grepp och göras en förnyad analys av reglernas samlade effekt för enskildas personliga integritet.

I ljuset av den senaste tidens reformer finns det också ett behov av att se över utformningen av myndigheternas och regeringens årliga redovisning av användningen av hemliga och preventiva tvångsmedel. Det är lämpligt att se över den frågan samlat i samband med att regleringen utvärderas.

Utredaren ska därför

- utvärdera tillämpningen och kartlägga behovet och nyttan av de utökade möjligheterna att använda hemliga och preventiva tvångsmedel,
- ta ställning till om det finns utrymme för förbättringar av reglerna så att de blir än mer träffsäkra i tillämpningen,
- ta ställning till om den reglering om preventiva tvångsmedel som upphör att gälla vid utgången av september 2028 bör gälla utan tidsbegränsning,
- göra en analys av den samlade regleringens konsekvenser för den personliga integriteten,
- ta ställning till hur den årliga redovisningen av användningen av hemliga och preventiva tvångsmedel ska ske, och
- lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder.

Uppdraget att analysera behovet och nyttan av samt föreslå en möjlighet att störa, sabotera och avbryta cyberbrott

Med en ökad digitalisering och ny teknik öppnas nya möjligheter för kriminalitet. Kriminella aktörer använder i större utsträckning avancerad teknologi för att begå brott. Det handlar inte bara om brott som begås helt digitalt, utan nästan alla brott har i dag en digital komponent.

Begreppet cyberbrott innefattar en mängd olika brott. Den gemensamma nämnaren för denna typ av brottslighet är att den begås i eller via cybermiljö. Det kan t.ex. handla om ransomware- eller överbelastningsattacker, försäljning av droger på marknadsplatser online, spridning av sexuellt övergreppsmaterial online, rekrytering av barn och unga till kriminella nätverk online, spionerи och olovlig underrättelseverksamhet. Brott i cybermiljö är ofta mycket svåra att avbryta och utreda. Det beror bl.a. på att brottsligheten är gränsöverskridande till sin natur men också på den utbredda användningen av anonymiseringstekniker som gör att det är svårt att identifiera misstänkta personer.

Cyberbrottsligheten utgör därmed ett växande hot mot både enskilda och den nationella säkerheten. Som exempel kan nämnas att Säkerhetspolisen i sin årsbok för 2023–2024 konstaterar att Sverige utgör en plattform för främmande makts cyberangrepp. Att hacka privatpersoners enheter och bygga upp kapacitet genom denna typ av infrastruktur möjliggör både cyberangrepp och inhämtning av information. Sett till världen i stort ligger Sverige högt när det kommer till mängden hackad infrastruktur som används för att begå förnekbara cyberangrepp. Totalt under de senaste åren rör det sig om tiotusentals hackade enheter i Sverige.

Utvecklingen har lett till att de brottsbekämpande myndigheterna inte har tillräckligt bra verktyg för att bekämpa brott i cybermiljö. När det gäller cyberbrottsligheten behöver de brottsbekämpande myndigheterna ändra strategi till att aktivt förhindra, störa, sabotera och avbryta brott för att minimera skada. Det kan t.ex. handla om att ta sig in i eller etablera sig i en viss digital miljö för att följa den brottsliga verksamheten eller att påverka, förändra eller sabotera den digitala miljön så att brottsligheten inte kan fortgå. Det finns exempel på att andra jämförbara länder infört en möjlighet för de brottsbekämpande myndigheterna att störa, sabotera och avbryta pågående cyberbrottslighet, något som visat sig vara ett effektivt verktyg.

Utredaren ska därför

- kartlägga och redovisa andra jämförbara länders rättsliga möjligheter att störa, sabotera och avbryta pågående cyberbrottslighet,
- analysera behovet och nyttan av samt föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö, eller vidta andra jämförbara åtgärder i sådan miljö, i syfte att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot och sabotera sådan brottslighet, och
- lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder.

Uppdraget att utreda vissa andra straffprocessrättsliga frågor av betydelse för det brottsbekämpande arbetet

En översyn av systemet med offentliga ombud

I ärenden om vissa hemliga och preventiva tvångsmedel och ärenden om anonyma vittnen hos domstol ska offentliga ombud bevaka enskildas integritetsintressen. Ett offentligt ombud har rätt att ta del av det som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut (27 kap. 26 § rättegångsbalken). Den person som kan komma i fråga som offentligt ombud ska vara eller ha varit advokat eller ha varit ordinarie domare. Därutöver måste ombudet vara svensk medborgare och får inte vara i konkurstillstånd eller ha förvaltare. Regeringen förordnar för tre år i taget personer som kan tjänstgöra som offentliga ombud.

De offentliga ombuden är en central del av det system med rättssäkerhetsgarantier som omger den hemliga och preventiva tvångsmedelsanvändningen. I takt med att det genomförts nya reformer har behovet av offentliga ombud ökat, både när det gäller ärenden om hemliga och preventiva tvångsmedel och ärenden om anonyma vittnen enligt lagen (2024:1180) om anonyma vittnen i brottmål. Med dagens reglering är det svårt att rekrytera tillräckligt många ombud med den efterfrågade kompetensen och den tillgänglighet som krävs. Systemet med offentliga ombud behöver därför ses över.

Utredaren ska därför

- analysera det samlade behovet av offentliga ombud,
- ta ställning till hur regleringen om offentliga ombud bör ändras för att tillgodose behovet och framför allt hur rekrytering av offentliga ombud bör ske framöver, t.ex. på vilket sätt rekryteringsbasen kan breddas samtidigt som tillräcklig kompetens upprätthålls, och
- lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder.

En möjlighet att neka enskilda att göra en egen inspelning av ett förhör

I ett av Justitieombudsmannens (JO) tillsynsärenden (JO:s ämbetsberättelse 2023 s. 280, dnr. 2837–2022) framkom att en man som skulle förhöras av polisen ville göra en egen ljudinspelning av förhöret med sin mobiltelefon. När han kontaktade polisen inför förhöret fick han information om att någon inspelning inte skulle tillåtas och att telefonen kunde tas om hand om han ändå gjorde en inspelning. JO konstaterade i sitt beslut att det inte finns någon författningsgrundad rätt för en enskild person att göra en egen inspelning av ett polisförhör, men inte heller något uttryckligt förbud mot det. Som utgångspunkt är det därför enligt JO tillåtet att göra en egen inspelning av ett förhör.

Samtidigt konstaterade JO att det i en förundersökning kan förekomma uppgifter som omfattas av sekretess och att det är angeläget att det som kommer fram vid ett förhör inte röjs för utomstående på ett sätt som kan medföra skada eller men för brottsutredningen eller andra skyddsvärda ändamål. Det finns också ett intresse av att kunna upprätthålla ordningen vid ett förhör och genomföra det på ett effektivt och ändamålsenligt sätt. Enligt JO kan en förhörsledare eller undersökningsledare redan i dag neka en person att göra en egen inspelning om det finns konkreta och sakligt godtagbara omständigheter av det slag som nu nämnts. Ett sådant ställningstagande ska dokumenteras. Precis som JO framhåller i sitt beslut talar rättssäkerhetsskäl för att en reglering i författning bör övervägas.

Utredaren ska därför

- analysera behovet och nyttan av samt ta ställning till om det bör införas en möjlighet att neka en person att göra en egen inspelning av ett förhör och att tillfälligt ta om hand elektronisk utrustning som kan användas för en sådan inspelning, och
- oavsett vilket ställningstagande som görs, lämna nödvändiga författningsförslag.

En misstänkts och dennes försvarares rätt att få en kopia av förundersökningsprotokollet i vissa fall

Så snart åtal väcks har den misstänkte och dennes försvarare rätt att få en papperskopia av förundersökningsprotokollet (23 kap. 21 a § första stycket rättegångsbalken). Rätten att få en sådan kopia gäller även när förundersökningsprotokollet innehåller uppgifter som omfattas av sekretess. Den misstänkte och försvararen har också rätt att på begäran få en kopia av handlingar som innehåller sådant som har förekommit vid förundersökningen och som inte ingår i förundersökningsprotokollet, s.k. sidomaterial. Det gäller dock inte om det exempelvis finns risk för att sekretessbelagda uppgifter obehörigen kommer att lämnas vidare (23 kap. 21 a § andra stycket rättegångsbalken). När den misstänkte eller försvararen får ta del av ett förundersökningsprotokoll eller en annan handling som innehåller sekretessbelagda uppgifter kan uppgifterna lämnas ut med sekretessförbehåll, dvs. med ett förbehåll om att uppgifterna inte får lämnas vidare (23 kap. 21 a § tredje stycket rättegångsbalken och 10 kap 4 § offentlighets- och sekretesslagen [2009:400]). Ett sådant förbehåll inskränker mottagarens rätt att förfoga över materialet och ålägger mottagaren tystnadsplikt. Den som inte följer villkoren i förbehållet utan sprider uppgifterna kan straffas för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken.

Säkerhetspolisen har i en hemställan (Ju2021/02556) framfört önskemål om att reglerna i 23 kap. 21 a § rättegångsbalken om rätten att få en papperskopia av förundersökningsprotokollet bör ses över mot bakgrund av att det i vissa fall kan finnas uppgifter i förundersökningsprotokollet som skulle kunna medföra men för Sveriges säkerhet om de röjs. Som exempel kan nämnas att det i en förundersökning om t.ex. spionerі eller olovlig underrättelseverksamhet mot Sverige kan finnas uppgifter som omfattas av försvarssekretess, dvs. uppgifter som kan antas skada landets försvar eller på annat sätt vålla fara för rikets säkerhet om de röjs (15 kap. 2 § offentlighets- och sekretesslagen). Det kan därmed finnas en risk för att sådana uppgifter sprids om de lämnas ut till den misstänkte, vilket inte bedöms kunna hanteras med hjälp av ett sekretessförbehåll. Det finns mot den bakgrunden skäl att överväga om reglerna om rätten till en kopia av förundersökningsprotokollet bör ändras för att hantera de risker som Säkerhetspolisen beskriver.

Utredaren ska därför

- analysera behovet och nyttan av samt ta ställning till om det bör införas en möjlighet att inskränka rätten för en misstänkt och dennes försvarare att få en kopia av förundersökningsprotokollet om det innehåller uppgifter som omfattas av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen, och
- oavsett vilket ställningstagande som görs, lämna nödvändiga författningsförslag.

Konsekvensbeskrivningar

I enlighet med förordningen (2024:183) om konsekvensutredningar och kommittéförordningen (1998:1474) ska utredaren redovisa en konsekvensutredning för de förslag som lämnas. Utredaren ska bedöma och redovisa förslagens ekonomiska och andra konsekvenser, t.ex. konsekvenserna för det brottsbekämpande arbetet och den personliga integriteten. Särskild vikt ska läggas vid effekter för rättsväsendets myndigheter.

Utredaren ska beskriva och, när det är möjligt, kvantifiera de samhällsekonomiska effekterna av de förslag som läggs. De offentligfinansiella effekterna av utredarens förslag ska beräknas. Om förslagen innebär offentligfinansiella kostnader ska förslag till finansiering lämnas enligt 15 § kommittéförordningen.

Utredaren ska även bedöma och redovisa hur förslagen förhåller sig till regeringsformen, mediegrundlagarna, EU-rätten inklusive EU:s rättighetsstadga samt Sveriges internationella åtaganden om mänskliga rättigheter inklusive barnkonventionen. Utredaren ska redovisa vilka konsekvenser som de förslag som lämnas har ur ett barnrättsperspektiv samt ur ett jämställdhetsperspektiv.

Arbetets genomförande, kontakter och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från de allmänna domstolarna, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden och Sveriges advokatsam-

fund men även andra berörda myndigheter och aktörer. Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och inom utredningsväsendet. Utredaren ska beakta utvecklingen vid såväl EU:s lagstiftande institutioner som EU-domstolen, Europadomstolen och Europarådet.

Utredaren ska säkerställa att en välfungerande systematik i övriga regelverk upprätthålls. Det innebär att utredaren även ska bedöma behovet av följdändringar, t.ex. i lagen om internationell rättslig hjälp i brottmål, lagen om en europeisk utredningsorder, brottsdatalagen (2018:1177) och kompletterande registerförfattningar samt lagen om särskild kontroll av vissa utlänningar. Viktiga ställningstaganden som gjorts vid utformningen av förslagen ska beskrivas. Vidare ska alternativa lösningar som övervägts beskrivas liksom skälen till att de har valts bort. Utredaren har även möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas under förutsättning att uppdraget ändå kan redovisas i tid. Utredaren ska emellertid inte lämna förslag som innebär att underrättelseverksamheten i övrigt regleras.

Uppdraget ska redovisas senast den 29 maj 2026.

(Justitiedepartementet)

Kommittédirektiv 2026:20

Tilläggsdirektiv till Utredningen om hemliga och preventiva tvångsmedel (Ju 2025:04)

Beslut vid regeringssammanträde den 26 mars 2026

Utvidgning av och förlängd tid för uppdraget

Regeringen beslutade den 20 februari 2025 kommittédirektiven Hemliga och preventiva tvångsmedel – en effektiv och tydlig reglering (dir. 2025:12). Syftet med utredningen är bl.a. att göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel för att åstadkomma en mer effektiv och tydlig reglering och förbättra möjligheterna att använda tvångsmedlen i brottsbekämpningens olika faser.

Utredaren får nu, utöver vad som framgår av de ursprungliga direktiven, i uppdrag att

- analysera och ta ställning till om ett tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation samt viss hemlig dataavläsning ska kunna knytas till en person,
- analysera och ta ställning till om preventiva tvångsmedel ska kunna användas i fler fall och utan koppling till en organisation eller grupp, och
- oavsett vilket ställningstagande som görs, lämna nödvändiga författningsförslag.

Utredningstiden förlängs. Enligt de ursprungliga direktiven skulle uppdraget redovisas senast den 29 maj 2026. Uppdraget ska i stället redovisas senast den 1 februari 2027.

Uppdraget att utreda och föreslå en möjlighet att knyta ett tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation samt viss hemlig dataavläsning till en person

Hemlig avlyssning och övervakning av elektronisk kommunikation kan användas vid en förundersökning och får endast avse ett telefonnummer, en annan adress (t.ex. en e-postadress) eller en viss elektronisk kommunikationsutrustning som har viss anknytning till den person som åtgärden avser (se t.ex. 27 kap. 18 a § tredje stycket rättegångsbalken). Vilket telefonnummer eller liknande som tvångsmedlet gäller ska anges i tillståndet (27 kap. 21 § tredje stycket rättegångsbalken). Hemlig avlyssning och övervakning av elektronisk kommunikation kan verkställas genom hemlig dataavläsning (4 § lagen [2020:62] om hemlig dataavläsning). Ett tillstånd till sådan hemlig dataavläsning kombineras ofta med ett tillstånd att hämta in andra uppgifter som är åtkomliga i ett avläsningsbart informationssystem, t.ex. sådana uppgifter som finns lagrade i en utrustning eller som visar hur utrustningen används. I ett tillstånd till hemlig dataavläsning ska det anges vilket avläsningsbart informationssystem som tillståndet gäller (18 § lagen om hemlig dataavläsning). Med ett avläsningsbart informationssystem avses en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst (1 § lagen om hemlig dataavläsning).

Hemlig avlyssning och övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter och andra uppgifter som är åtkomliga i ett avläsningsbart informationssystem kan också användas i de brottsbekämpande myndigheternas underrättelseverksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar vissa allvarliga brott (s.k. preventiva tvångsmedel). De preventiva tvångsmedlen regleras i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen), lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen om hemlig dataavläsning. Tvångsmedlen kan därtill användas i utlänningsärenden med kvalificerade säkerhetsaspekter med stöd av lagen (2022:700) om särskild kontroll av vissa utlänningar.

Hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter. Hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter kan också användas för att lokalisera personer som håller sig undan verkställighet av beslut om anhållande och häktning eller av frihetsberövande påföljd med stöd av bl.a. lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

Hemliga och preventiva tvångsmedel får sedan den 1 oktober 2025 användas mot barn under 15 år för att förebygga, förhindra, upptäcka och utreda vissa allvarliga brott med stöd av bl.a. lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Frågor om hemliga och preventiva tvångsmedel prövas som huvudregel av domstol på ansökan av åklagaren (se t.ex. 27 kap. 21 § rättegångsbalken). Beslut om inhämtning enligt inhämtningslagen fattas dock av åklagare vid Åklagarmyndigheten på ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket (3 § inhämtningslagen). Domstolen måste i vissa fall hålla ett sammanträde när den prövar frågor om hemliga och preventiva tvångsmedel (jfr t.ex. 27 kap. 28 och 28 a §§ rättegångsbalken). Det finns också ett visst utrymme för åklagaren att fatta interimistiskt beslut om hemliga och preventiva tvångsmedel i brådskande fall (se t.ex. 27 kap. 21 a § rättegångsbalken).

Kriminella sätter i dag i system att byta t.ex. telefon eller användarkonto för att undvika att bli föremål för avlyssning eller övervakning. Varje gång ett sådant byte sker måste ett nytt beslut meddelas av domstolen, eftersom det i beslutet måste anges vilket telefonnummer eller liknande som tillståndet omfattar. När den verkställande myndigheten behöver invänta ett nytt beslut kan det uppstå ett glapp i avlyssningen som kan leda till informationsförluster. Komplexiteten i den mobila telefonin och nätverksteknologin ställer därtill andra krav på lagstiftningen än vad den fasta telefonin en gång gjorde. I dag är det fråga om flera lager av adresser som är kopplade både till ett sim-kort och till själva utrustningen (t.ex. en mobiltelefon). Adresserna genererar olika uppgifter i näten och för en användare går det att växla fram och tillbaka mellan olika adresser med ett knapptryck. Ett sätt att förenkla tillståndsförfarandet är att i stället knyta tillståndet till en person. Sådana möjligheter finns redan

i Danmark och Finland. Att knyta tillståndet till en person kan också innebära en mer teknikneutral reglering som kan stå sig över tid.

I svensk rätt finns det en möjlighet att knyta ett tillstånd till hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning som gäller motsvarande uppgifter till en person i stället för till en plats. Det gäller både när tvångsmedlen används i en förundersökning och när de används i de brottsbekämpande myndigheternas underrättelseverksamhet. Riksdagen har tillkännagett för regeringen det som utskottet anför om att ett tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation bör kunna knytas till en person (bet. 2021/22:JuU24 punkt 14, rskr. 2021/22:216).

Frågan om att knyta ett tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation samt viss hemlig dataavläsning till en person har utretts tidigare, senast av Utredningen om tvångsmedel mot underåriga (Ju 2023:12). Utredningen överlämnade i december 2024 betänkandet Effektivare verktyg för att bekämpa brott av unga lagöverträdare (SOU 2024:93) till regeringen. I betänkandet föreslås att det, i stället för att införa en möjlighet att knyta tvångsmedelstillstånden till en person, ska införas ett snabbare beslutsförfarande för tvångsmedlen där särskilt utpekade befattningshavare inom polisen får besluta om ett s.k. tillfälligt tvångsmedelstillstånd. Förslaget har kritiserats av remissinstanserna ur olika aspekter och regeringen avser inte att gå vidare med förslaget. Frågan om att knyta tvångsmedelstillstånden till en person är fortsatt mycket angelägen för de brottsbekämpande myndigheterna.

En ordning där tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation samt viss hemlig dataavläsning knyts till en person skulle innebära att en ny övervakning, avlyssning eller avläsning kan påbörjas betydligt snabbare än i dag. På så sätt skulle informationsförlusten som uppstår när kriminella t.ex. byter telefonnummer minska, vilket i sin tur skulle kunna leda till en mer effektiv brottsbekämpning.

Utredaren ska därför

- analysera och ta ställning till om tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation ska kunna knytas till en person, i stället för ett telefonnummer, en annan adress eller en viss elektronisk kommunikationsutrustning vid en brottsutredning,

- analysera och ta ställning till om tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter eller andra uppgifter som är åtkomliga i ett avläsningsbart informationssystem ska kunna knytas till en person i stället för ett avläsningsbart informationssystem vid en brottsutredning,
- analysera och ta ställning till om tillstånd till sådana tvångsmedel som anges i föregående punkter ska kunna knytas till en person när tvångsmedlen används i de brottsbekämpande myndigheternas underrättelseverksamhet, i utlänningsärenden med kvalificerade säkerhetsaspekter samt – i relevanta delar – för att lokalisera en person som håller sig undan verkställighet av beslut om anhållande och häktning eller av frihetsberövande påföljd, och
- oavsett vilket ställningstagande som görs, lämna nödvändiga författningsförslag.

Uppdraget att utreda och föreslå en möjlighet att använda preventiva tvångsmedel i fler fall

Preventiva tvångsmedel används i de brottsbekämpande myndigheternas underrättelseverksamhet för att upptäcka, förebygga och förhindra viss särskilt allvarlig brottslig verksamhet. Regleringen av de preventiva tvångsmedlen finns bl.a. i preventivlagen. Tidigare tillämpades preventivlagen nästan uteslutande av Säkerhetspolisen i fråga om t.ex. spioneri- och terroristbrott. I oktober 2023 utvidgades preventivlagens tillämpningsområde till att avse även vissa särskilt allvarliga brott som förekommer inom kriminella nätverk och som hanteras av Polismyndigheten och Tullverket, t.ex. mord, allmänfarlig ödeläggelse och allvarliga narkotika- och smugglingsbrott. Bestämmelserna som utvidgar preventivlagens tillämpningsområde är tidsbegränsade och upphör att gälla vid utgången av september 2028.

För att tvångsmedel enligt preventivlagen ska få användas inom det utvidgade tillämpningsområdet krävs att det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet som innefattar vissa särskilt angivna brott och att det kan befaras att en person, som tillhör eller verkar för organisationen eller gruppen, medvetet kommer att främja den brottsliga

verksamheten (se t.ex. 1 a § preventivlagen). Det utvidgade tillämpningsområdet innefattar alltså inte brottslig verksamhet som utövas av en person utan koppling till den organisation eller grupp där den brottsliga verksamheten kommer att utövas. Ett exempel på en situation som enligt nuvarande ordning i vissa fall riskerar att falla utanför preventivlagens tillämpningsområde kan ses inom brottsfenomenet ”crime as a service”. Brottsfenomenet kännetecknas av att grova brott, t.ex. sprängningar och skjutningar, utannonseras och koordineras av kriminella aktörer i olika digitala tjänster där den eller de personer som anlitas för att utföra gärningen eller en del av gärningen saknar direkt koppling till uppdragsgivaren. Inte sällan är det fråga om mycket unga personer som anlitas för att utföra mord- eller sprängningsuppdrag. Andra exempel på grova brott som sker utan anknytning till en organisation eller grupp, och som därmed faller utanför preventivlagens tillämpningsområde, är det dödliga våldet i nära relationer som framför allt drabbar kvinnor och allvarliga sexualbrott mot barn. Det kan också handla om vansinnesdåd eller brott som utförs av ensamagerande gärningsmän, t.ex. skolskjutningar. Ett verktyg för att förbättra möjligheterna att förhindra sådant mycket allvarligt våld skulle kunna vara att använda preventiva tvångsmedel i fler fall och utan koppling till en organisation eller grupp.

Utredaren ska därför

- analysera och ta ställning till om preventiva tvångsmedel ska kunna användas i fler fall och utan koppling till en organisation eller grupp, och
- oavsett vilket ställningstagande som görs, lämna nödvändiga författningsförslag.

Redovisning av uppdraget

Utredningstiden förlängs. Enligt de ursprungliga direktiven skulle uppdraget redovisas senast den 29 maj 2026. Uppdraget ska i stället redovisas senast den 1 februari 2027.

Utredaren har även fortsättningsvis möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas inom ramen för utredningen under förutsättning att uppdraget ändå kan redovisas i tid.

(Justitiedepartementet)

Kommittédirektiv 2026:40

Tilläggsdirektiv till Utredningen om hemliga och preventiva tvångsmedel (Ju 2025:04)

Beslut vid regeringssammanträde den 28 maj 2026

Förkortad tid för en del av uppdraget

Regeringen beslutade den 20 februari 2025 kommittédirektiven Hemliga och preventiva tvångsmedel – en effektiv och tydlig reglering (dir. 2025:12). Syftet med utredningen är bl.a. att göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel för att åstadkomma en mer effektiv och tydlig reglering och förbättra möjligheterna att använda tvångsmedlen i brottsbekämpningens olika faser. Utredningsuppdraget innefattar också att analysera behovet och nyttan av samt föreslå en möjlighet att störa och avbryta cyberbrott. Uppdraget skulle enligt de ursprungliga direktiven redovisas senast den 29 maj 2026. Regeringen beslutade den 26 mars 2026 tilläggsdirektiv till utredningen där uppdraget utvidgades och utredningstiden förlängdes till den 1 februari 2027 (dir. 2026:20).

Uppdraget att analysera behovet och nyttan av samt föreslå en möjlighet att störa, sabotera och avbryta cyberbrott ska redovisas i ett delbetänkande och utredningstiden i den delen förkortas. Uppdraget ska i den delen redovisas senast den 30 juni 2026.

(Justitiedepartementet)

Statens offentliga utredningar 2026

Kronologisk förteckning

1. Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. Fi.
2. 710 miljoner skäl till reformer. Ju.
3. Genomförande av plattformsdirektivet. A.
4. Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. U.
5. Utvidgad avdragsrätt för sponsring m.m. Fi.
6. En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. S.
7. Förstärkt uppföljning och utvärdering av folkhälsopolitiken.
   Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser.
   Del II: Utvärdering av alkoholpolitikens styrmedel. S.
8. Rättssäker samhällsvård för barn och unga. S.
9. Registrering av EES-medborgare. Ju.
10. Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. Ju.
11. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
12. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
13. Straffansvar för deltagande i och samröre med kriminella sammanslutningar. Ju.
14. Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. KN.
15. Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. Ku.
16. Försvarsexportinitiativ. För gemensam säkerhet. Fö.
17. Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. LI.
18. Odlingstorv och klimatet. Fi.
19. Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. S.
20. Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. Fi.
21. Återkallelse av svenskt medborgarskap. Ju.
22. Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. S.
23. Tolkavgift och förbud mot barntolkning. A.
24. Mervärdesskatt vid uthyrning och överlåtelse av fastighet. Fi.
25. Ett smittskydd för framtiden. S.
26. Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. Ju.
27. Lättnader i kraven på hållbarhetsrapportering. Ju.
28. Tillgång till passageraruppgifter i brottsbekämpningen. Ju.
29. Förbud mot uppfödning av djur för pälsproduktion. LI.
30. Mer flexibla regler om verkställighet av häktning och fängelsestraff. Ju.
31. Ett investeringsprogram för kultur. Ku.
32. Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. KN.
33. Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. KN.

34. Nya nätbrott och andra åtgärder för genomförandet av direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Volym 1 & 2. Ju.
35. En åldersgräns för barns tillgång till sociala medier. S.
36. Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. S.
37. Förutsättningar för en likvärdig och språkutvecklande förskola. U.
38. Behovsstyrd vård. S.
39. Ett nytt system för återkrav inom socialförsäkringen. S.
40. Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. KN.
41. Jämställdhet i en föränderlig tid – nuläge och vägar framåt. Volym 1 & 2. A.
42. Ett nytt regelverk för granskning av utländsk finansiering av trossamfund och andra verksamheter. Volym 1 och 2. Ju.
43. Åtgärder mot överskuldsättning. Fi.
44. En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning. Fi.
45. Effektiva ingripanden mot brott i cybermiljö. Ju.

Statens offentliga utredningar 2026

Systematisk förteckning

Kulturdepartementet

Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. [15]

Ett investeringsprogram för kultur. [31]

Landsbygds- och infrastrukturdepartementet

Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. [17]

Förbud mot uppfödning av djur för pälsproduktion. [29]

Socialdepartementet

En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. [6]

Förstärkt uppföljning och utvärdering av folkhälsopolitiken. Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser. Del II: Utvärdering av alkoholpolitikens styrmedel. [7]

Rättssäker samhällsvård för barn och unga. [8]

Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. [19]

Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. [22]

Ett smittskydd för framtiden. [25]

En åldersgräns för barns tillgång till sociala medier. [35]

Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. [36]

Behovsstyrd vård. [38]

Ett nytt system för återkrav inom socialförsäkringen. [39]

Utbildningsdepartementet

Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. [4]

Förutsättningar för en likvärdig och språkutvecklande förskola. [37]