Datum: 2026-11-09
Diarienummer Ju2026/01670
Justitiedepartementet
ju.remissvar@regeringskansliet.se

Betänkandet "Effektiva ingripanden mot brott i cybermiljö" SOU 2026:45

DFRI, Föreningen för Digitala Fri- och Rättigheter, lämnar följande synpunkter

Lagen ger de brottsbekämpande myndigheterna rätt att begå det som annars skulle vara dataintrång, utan att säkerställa tillräcklig insyn eller rättsmedel för de drabbade, och utan att tröskeln för ingripande är knuten till en brottsmisstanke.

Operatörssamarbetet regleras på ett sätt som kombinerar utvidgad tystnadsplikt med avsaknad av fungerande mekanismer för att säkerställa samarbete – vare sig incitament, sanktioner eller verifieringsmöjligheter.

Lagen reglerar inte hur myndigheterna ska förvärva de verktyg som behövs för ingripandena. Eftersom systemskydd får brytas och sårbarheter får utnyttjas öppnas dörren för att staten köper exploits och åtkomst på kriminella marknader med skattemedel.

Dataintrång legaliseras

Utredningen konstaterar själv att de åtgärder som behövs för att ingripa i cybermiljö normalt är kriminaliserade (s197), men att en myndighet kan vidta åtgärder "*utan att göra sig skyldiga till dataintrång*" (s21). Till skillnad från traditionella tvångsmedel som hemlig avlyssning enligt 27 kap. 18 § rättegångsbalken, vilka förutsätter misstanke om konkret brott, får ingripanden enligt den föreslagna lagen vidtas redan "*om det kan antas att ett informationssystem utnyttjas i brott eller brottslig verksamhet i cybermiljö*" (s42).

Enligt 17 § i förslaget får "*systemskydd får brytas eller kringgås och tekniska sårbarheter får utnyttjas*" (s45), genom "*både genom avancerade tekniska åtgärder och genom enklare metoder, som inloggning med användarnamn och lösenord eller byte av lösenord*" (s25). Utredningen beskriver också hur systemskydd ska kringgås, genom att "*installera ett särskilt program*" och på så sätt "ta sig förbi en multifaktorautentisering" (s307).

DFRI noterar att denna bestämmelse innebär att staten aktivt ska utnyttja säkerhetsbrister i stället för att rapportera och åtgärda dem. Detta strider mot såväl cybersäkerhetslagen (2025:1506) som syftet med NIS 2-direktivet (2022/2555), vilka båda syftar till att stärka skyddet av informationssystem.

Enligt 2 kap. 3 § cybersäkerhetslagen (2025:1506) ska verksamhetsutövare "*vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem*". Säkerhetsåtgärderna ska "*utgå från ett allriskperspektiv*" och omfatta bland annat "*incidenthantering*", "*säkerhet i leveranskedjan*" samt "*strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna*". En statlig politik som å ena sidan kräver att operatörer skyddar sina system och å andra sidan ger myndigheterna rätt att penetrera dem, detta skapar ett systematiskt säkerhetsproblem.

DFRI anser att lagen måste innehålla en samordningsmekanism med Nationellt cybersäkerhetscenter (NCSC) för att säkerställa att utnyttjade sårbarheter skyndsamt rapporteras och täpps till efter avslutat ingripande.

Konstitutionellt skydd för den personliga integriteten

DFRI anser att förslaget inte i tillräcklig grad analyserar konsekvenserna för det grundlagsskyddade skyddet mot integritetsintrång enligt 2 kap. 6 § regeringsformen.

Tekniska ingripanden i informationssystem kan ge tillgång till stora mängder personuppgifter och kommunikation och uppgifter som saknar relevans för den brottslighet som föranlett ingripandet. Ett ingripande kan påverka andra användare av samma system, utan att dessa personer är misstänkta för brott eller känner till att ett ingripande har ägt rum.

Det är därför inte tillräckligt att bedöma proportionaliteten utifrån den misstänkte personen eller det informationssystem som är föremål för myndighetens intresse. Även konsekvenserna för tredje man och risken för insamling av ovidkommande personuppgifter måste beaktas.

Utredningen ser problemet men tar inte konsekvenserna av det. Den anger att ingripandet kan rikta sig mot "ett informationssystem som är tillgängligt för flera personer" och mot "en begränsad del av ett större informationssystem, exempelvis ett användarkonto" (s309). Svaret på den invändningen är 18 §, som kräver att påverkan på "annan som använder samma del av informationssystemet blir så begränsad som möjligt" (s308). Men regeln ska enligt utredningen själv inte tillämpas när det är "syftet med att direkt påverka andras användning av ett informationssystem",exempelvis vid blockering av en marknadsplats (s309, s418) – då är skadan för tredje man avsiktlig och utan begränsning. Underrättelse saknas också: "det finns inget generellt behov av att underrätta enskilda" (s317), och de drabbade får varken information eller rättsmedel.

Att detta inte är en teoretisk risk visar betänkandet själv: sökning efter en server kan medföra "nedstängning av verksamhet som inte är illegal och därmed drabba utomstående i större utsträckning" (s313), och frågan om värdtjänstbolagens medverkan "ligger utanför utredningens direktiv" (s314). Inte heller den skada staten själv orsakar hanteras: kravet på att systemet ska lämnas i ett tillstånd minst lika säkert som före ingripandet avfärdas utan ersättning (s308).

DFRI anser därför att lagen bör innehålla ett uttryckligt krav på att myndigheten innan beslut upprättar en specifik konsekvensanalys för tredje man (en sidoskadeanalys). Dessutom krävs en strikt skadeståndsregel som garanterar att utomstående aktörer kompenseras fullt ut för de ekonomiska skador som driftstopp eller blockeringar orsakar.

Förebyggande åtgärder har dokumenterad effekt

Utredningen innehåller ingen kvantifierad effektberäkning, utan skriver istället att nyttan "*med fog förväntas leda till ökad samhällsnytta*" (s195) och att "*De samhällsekonomiska vinsterna av förslagen är ännu svårare att beräkna än kostnaderna. Utredningen avstår därför från att försöka kvantifiera dem*" (s377).

Till skillnad från de föreslagna ingripandena är förebyggande åtgärder mätbara; att övergången till tvåfaktorsautentisering har gett tydliga resultat visar både Microsofts Digital Defense Report 2024 och BRÅ:s nationella trygghetsundersökning.

Staten riskerar att finansiera marknaden för intrångsverktyg

Marknaden för sådana verktyg är inte hypotetisk, och betänkandet beskriver den själv. "*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*" (s132). Bland erbjudandena nämns "*erbjudanden om initiala åtkomstuppgifter" och "kriminella tjänster, inklusive prenumerationer på verktyg som används för att utnyttja sårbarheter i programvara, operativsystem och förfalskningstjänster*" (s133). Betänkandet beskriver samtidigt cyberbrottsligheten som "*alltmer industrialiserad, organiserad och tekniskt avancerad*", med "k*riminella nätverk som agerar i en struktur som går att jämföra med professionella företag med egna tjänster, leveranskedjor och internationella samarbeten*" (s133).

En ej reglerad andel av den budgeterade miljarden skattekronor kan alltså komma att gå till finansiera den brottslighet som lagen ska motverka. En myndighet som betalar för nolldagssårbarheter ökar både efterfrågan och tillgången till just nolldagssårbarheter, vilket gör det mindre attraktivt för forskare att rapportera sårbarheter vidare till leverantören. Det strider mot den logik som NIS 2-direktivets artikel 12.1 och cybersäkerhetslagen vilar på, och mot betänkandets egen statistik om att nolldagssårbarheter utgjorde 62 procent av allt observerat utnyttjande under januari-augusti 2026.

Det saknas garantier för att skattemedel inte indirekt finansierar aktörer i den grå eller svarta sårbarhetsekonomin. Lagen bör därför kompletteras med ett uttryckligt förbud mot att köpa eller använda verktyg vars ursprung inte kan spåras till legitima, granskade säkerhetsföretag.

Dokumentation är inte samma sak som granskning

DFRI anser att utredningens krav på dokumentation inte är tillräckligt för att säkerställa rättssäkerheten och ansvarsutkrävanden.

Att en myndighet dokumenterar sina egna beslut och åtgärder innebär inte att dessa blir föremål för granskning. Dokumentationen visar inte heller i sig att ingripandet var nödvändigt, proportionerligt eller tekniskt korrekt genomfört.

De föreslagna befogenheterna kan innebära att myndigheter kringgår säkerhetsskydd, manipulerar informationssystem och påverkar uppgifter som tillhör personer utanför den aktuella brottsutredningen. Det ställer särskilt höga krav på extern granskning.

DFRI anser att tillsynen bör vara den som redan finns. Betänkandet föreslår att Myndigheten för säkerhet och integritetsskydd utövar tillsyn över den nya lagen (s333). Tillsynen måste dock kunna granska mer än beslutens rättsliga form. Nämnden måste ha tillgång till beslutsunderlaget och dokumentationen över det tekniska genomförandet utan att granskningen är beroende av den ingripande myndighetens bedömning av vilket material som får lämnas ut, och tillsynen måste omfatta det tekniska genomförandet. Varje ingripande bör dessutom anmälas till nämnden, så att tillsynen blir systematisk och inte enstaka fall; i dag föreslås underrättelse endast för interimistiska beslut om radering (s325).

Den enskilde måste kunna få sin fråga prövad. Betänkandet menar att ingripandena normalt görs öppet och att någon kontrollmöjlighet inte behövs (s338), men konstaterar samtidigt att det "inte kan garanteras att den som har varit utsatt för ingripandet får kännedom om det" (s333). DFRI

föreslår därför att nämndens kontrollmöjlighet enligt 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet utvidgas till att omfatta ingripanden enligt den nya lagen.

Lagen behöver inte räkna upp tillsynens uppgifter. Det räcker att den anger att tillsynen ska säkerställa att ingripanden görs enligt lagen och hur de genomförs, exempelvis om det fanns rättsliga förutsättningar för ingripandet och om en åtgärd som inneburit blockering eller radering begränsats till vad som var nödvändigt. Nämnden får själv bestämma vad tillsynen ska omfatta (s337), och tillsynen bör omfatta även påverkan på tredje man.

DFRI anser vidare att det bör införas krav på regelbunden offentlig redovisning av ingripandens omfattning, metoder och konsekvenser. Redovisningen bör ske på en aggregerad nivå för att inte röja pågående utredningar.

Operatörer hindras från att informera sina kunder

Utredningen föreslår att operatörers tystnadsplikt enligt 9 kap. 32 § lagen (2022:482) om elektronisk kommunikation (LEK) ska utvidgas till att omfatta även en begäran om medverkan enligt den nya lagen (s. 361). Den nya lagen ger myndigheterna ytterligare skäl att begära medverkan i tysthet.

Experterna uttrycker samma sak: "*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*" (s431).

Kraven enligt Europakonventionen

DFRI anser att förslaget behöver analyseras närmare med bakgrund av artiklarna 8 och 13 i Europakonventionen.

Artikel 8 skyddar den enskildes privatliv och korrespondens. Tekniska ingripanden som innebär åtkomst till, förändring av eller blockering av information i ett informationssystem kan utgöra intrång i dessa rättigheter. Sådana intrång måste vara lagliga, nödvändiga och proportionerliga samt skyddas av tillräckliga rättssäkerhetsgarantier.

Artikel 13 aktualiserar frågan om den enskilde har tillgång till ett effektivt rättsmedel när ett ingripande har inneburit en kränkning av konventionsskyddade rättigheter.

Operatörernas medverkan är i princip frivillig och blir olaglig att deklarera

Betänkandet innehåller ingen uttrycklig sanktion för en operatör som vägrar medverka, lämnar oriktiga uppgifter om vilka verktyg som finns tillgängliga, eller "glömmer" att nämna administrativa verktyg som skulle vara relevanta för ingripandet. Det finns inte heller någon rätt för polisen att granska operatörens interna system för att verifiera vilka verktyg som existerar.

Utredningen beskriver själv konsekvensen av uteblivet samarbete på följande sätt (s310):

"*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 och i förlängningen till "*större risker för*

informationssäkerheten och den personliga integriteten än vad som annars hade uppstått" (s311, med utredningens hänvisning till prop. 2019/20:64 s178).

Denna passus illustrerar det grundläggande problemet: operatörens samarbetsvilja är avgörande för att lagen ska fungera, men lagen innehåller inga mekanismer för att säkerställa sådant samarbete.

Ersättningen till operatörerna är det enda ekonomiska incitamentet i förslaget, och den är sparsamt reglerad. Enligt 20 § andra stycket har "*den som medverkar … rätt till ersättning för kostnader som uppstår vid sådan medverkan*" och "*ersättningen ska betalas av den ingripande myndigheten*" (s46). Motiveringen anger att myndigheten bör betala ersättning "f*ör sådana faktiska kostnader som uppstår vid medverkan*" (s312).

Betänkandet innehåller ingen regel om bokföring, skatt, kontrolluppgifter eller revision av den ersättning som betalas ut. Det är ett verkligt problem, eftersom betalningen för den som medverkar är en inkomst. Enligt 15 kap. 1 § inkomstskattelagen (1999:1229) ska "*ersättningar för varor, tjänster och inventarier, avkastning av tillgångar, kapitalvinster samt alla andra inkomster i näringsverksamheten*" tas upp som intäkt, och enligt 4 kap. 1 § bokföringslagen (1999:1078) ska ett företag "*löpande bokföra alla affärshändelser*".

För att lösa denna konstitutionella konflikt måste lagförslaget kompletteras med ett uttryckligt undantag från tystnadsplikten, vilket ger operatörens revisorer och ekonomipersonal rätt att ta del av underlaget i den utsträckning som krävs för att fullgöra skyldigheter enligt bokföringslagen.

Frivilligt samarbete bör inte regleras i lag

DFRI anser att frivilligt samarbete mellan operatörer och brottsbekämpande myndigheter inte bör regleras i 2000 ord mer lagtext. Skälen är flera:

a) Undergrävt förtroende för digitala tjänster.

b) Falsk bild av rättssäkerhet.

c) Brist på demokratisk förankring.

d) Undergrävande av kryptering och säkerhet. Om operatörer tvingas bistå med tekniska ingripanden uppstår en press att bygga in bakdörrar eller försvaga den generella nätverkssäkerheten för att underlätta myndigheternas åtkomst. Detta skapar sårbarheter som i förlängningen kan utnyttjas av fientliga aktörer.

DFRI tycker att

- Operatörer borde ha rätt att frivilligt samarbeta med brottsbekämpande myndigheter

- Kunder bör ha rätt att välja operatör efter deras deklarerade policy i sådana här frågor.

Föreningen för Digitala Fri- och Rättigheter, DFRI, gm

Christian Häggström, styrelseledamot

Bengt Jonsson (medlem i DFRI)
Tomas Forslund (medlem i DFRI)
Mats Karlsson (medlem i DFRI)
”ByteVis” (medlem i DFRI)

https://dfri.se , e-post styrelse@dfri.se