INTERNET STIFTELSEN

2026-11-09

Justitiedepartement

Ju2026/01670

Internetstiftelsens remissvar på Effektiva ingripanden mot brott i cybermiljö

Stiftelsen för Internetinfrastruktur (”Internetstiftelsen”) har beretts tillfälle att yttra sig över Effektiva ingripanden mot brott i cybermiljö (SOU 2026:45)

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation som verkar för ett internet som bidrar positivt till människor och samhälle. Organisationen säkerställer en robust och säker internetinfrastruktur som möter dagens och framtidens behov i Sverige, samtidigt som de främjar forskning, utbildning och undervisning med inriktning på internet.

Internetstiftelsen ansvarar för internets svenska toppdomän .se samt drift och administration av toppdomänen .nu. Intäkterna från denna verksamhet finansierar allmännyttiga insatser.

Genom satsningarna bidrar Internetstiftelsen till att öka den digitala kompetensen och resiliensen i samhället, stärka kunskapen om internetanvändning och dess påverkan på individ och samhälle samt utveckla identitets- och behörighetslösningar som förenklar inloggning och stärker säkerheten.

Internetstiftelsens vision är att alla i Sverige vill, vågar och kan använda internet.

Sammanfattning

Internetstiftelsen delar utredningens bedömning att brottsbekämpande myndigheter behöver effektiva och ändamålsenliga verktyg för att förhindra, störa och avbryta allvarlig brottslighet i cybermiljö. Vi har därför inget att invända mot lagstiftningens övergripande syfte. Internetstiftelsen anser dock att lagförslagets potentiella konsekvenser för internets säkerhet, stabilitet och funktion inte har analyserats i tillräcklig utsträckning.

Digitala informationssystem är ofta tekniskt sammanlänkade och bygger på gemensamma resurser och infrastrukturella beroenden. Ett ingripande som riktas mot ett visst system eller en viss användare kan därför få konsekvenser långt utanför det avsedda målet och påverka andra användare, tjänster och samhällsviktiga funktioner. Särskild hänsyn behöver tas till internets grundläggande infrastruktur, såsom domännamnssystemet (DNS), där även begränsade ingripanden kan medföra omfattande spridningseffekter.

Internetstiftelsen anser att dessa systemrisker tydligare måste beaktas vid proportionalitetsbedömningen. Det behöver säkerställas att ingripanden kan genomföras med tillräcklig teknisk precision, utan oproportionerlig påverkan på tredje man eller risk för kvarstående säkerhetsproblem. Lagförslagets teknikneutralitet bör

därför kompletteras med tydligare krav på dokumenterade, teknikoberoende och riskbaserade bedömningar inför beslut och verkställighet. Det behövs även en tydligare reglering av hur tekniska sårbarheter får utnyttjas och hanteras samt hur ingripanden ska avgränsas, avbrytas och återställas. Även risker för överblockering, fragmentering och minskad tillit till internet behöver beaktas.

Utredningen föreslår flera rättssäkerhetsgarantier, däribland krav på proportionalitet, aktsamhet, dokumentation och tillsyn. Internetstiftelsen bedömer dock att dessa inte i tillräcklig utsträckning säkerställer att de särskilda riskerna för internets tekniska funktion och stabilitet identifieras, bedöms och hanteras.

Internetstiftelsen kan mot denna bakgrund inte tillstyrka lagförslaget i dess nuvarande utformning.

Inledning

Internetstiftelsen är en infrastrukturaktör som värnar om en stabil, säker och tillförlitlig internetinfrastruktur. Vi har inget att invända mot lagstiftningens övergripande syfte, men kan inte tillstyrka förslaget innan nedan aspekter har analyserats och vid behov reglerats närmare.

Avsnitt 12 Överväganden om ingripanden i cybermiljö

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.

Internetstiftelsen delar problembilden att med ökad digitalisering och ny teknik öppnas nya möjligheter för kriminalitet. Brottslighet i form av olika typer av digitala angrepp utgör ett växande samhällshot. Vi delar vidare utredningens utgångspunkt att brottsbekämpande myndigheter behöver ändamålsenliga möjligheter att förhindra, störa och avbryta allvarlig brottslighet i cybermiljö. Vi ifrågasätter inte heller det behov som de relevanta myndigheterna har lyft.

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.

Internetstiftelsen anser dock att analys och bedömning av teknisk påverkan som det föreslagna lagförslaget kan medföra är otillräcklig. Vi utvecklar resonemanget nedan.

Avsnitt 14 Olika former av ingripanden

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.

Internetstiftelsen saknar en tillräcklig bedömning av hur de systemrisker som ett ingripande kan medföra ska vägas in i proportionalitetsprövningen. Eftersom åtgärder kan riktas mot gemensamt använda servrar, konton och internetbaserade tjänster kan konsekvenserna sträcka sig utanför det avsedda målet och påverka andra användare, beroende informationssystem samt relaterade funktioner. Ändringar av autentiseringsuppgifter, blockering av data eller installation av tekniska hjälpmedel kan

dessutom få kvarstående effekter på systemens riktighet, tillgänglighet och konfidentialitet. Proportionalitetsbedömningen bör därför uttryckligen omfatta risken för spridningseffekter, påverkan på tredje man och följdverkningar i gemensamt använd digital infrastruktur.

Det framgår inte uttryckligen av förslaget att ingripanden innefattar påverkan på DNS, men vi vill dock lyfta en möjlig risk avseende påverkan på DNS. Särskild hänsyn måste tas till ingripanden som kan påverka internets grundläggande funktioner såsom domännamnssystemet (DNS). Sådana funktioner utgör en förutsättning för att ett stort antal andra informationssystem och samhällsviktiga tjänster ska fungera. Ett ingripande i en del av infrastrukturen, även ett kortvarigt ingripande, kan därför få konsekvenser som är oproportionerliga i förhållande till det enskilda ingripandets syfte. Om DNS riskerar att påverkas måste denna risk uttryckligen ingå i proportionalitets-bedömningen.

Avsnitt 18 Verkställighet

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.

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.

Att *bereda sig tillgång till informationssystem* är en mycket bred och ospecificerad skrivning. Det avgörande är inte bara om ett ingripande tekniskt kan genomföras. Det måste också kunna visas att det kan genomföras med tillräcklig precision, med kontrollerbara konsekvenser, utan oproportionerlig påverkan på andra system och användare, utan att skapa nya eller kvarstående säkerhetsrisker samt med en realistisk plan för avbrytande, återställning och incidenthantering.

Möjligheten att kringgå systemskydd, utnyttja sårbarheter eller installera tekniska hjälpmedel för åtkomst till informationssystem kan medföra risker för att även andra användares uppgifter och system påverkas. Dessa risker blir särskilt betydande när informationssystem används gemensamt av många aktörer. I moderna digitala miljöer behandlas uppgifter från ett stort antal användare ofta inom gemensamma tekniska resurser. En åtkomst som är avsedd att träffa en viss användare eller ett visst informationssystem kan därför, beroende på systemets arkitektur och åtkomstkontroller, även möjliggöra åtkomst till andra användares information eller påverka andra tjänsters funktion.

Internetstiftelsen anser vidare att möjligheten att utnyttja tekniska sårbarheter måste förenas med en tydlig ordning för bedömning, dokumentation och hantering av de säkerhetsrisker som följer av detta. Det behöver särskilt klarläggas hur intresset av att utnyttja en sårbarhet för brottsbekämpning ska vägas mot intresset av att sårbarheten åtgärdas och därmed inte längre kan utnyttjas av andra aktörer.

Teknikneutraliteten bör kompletteras med en tydligt reglerad, teknikoberoende och riskbaserad metodik för beslut och verkställighet. En sådan metodik bör bedöma teknisk genomförbarhet och systemrisker, belysa påverkan på oskyldiga användare och tredje man och analys av risker för fragmentering, överblockering och minskad tillit.

19.4 En tidsbegränsad lag
Utredningens förslag: Den nya lagen ska tidsbegränsas till att gälla i fem år.

Om lagstiftningen genomförs, tillstyrker Internetstiftelsen att lagen ska tidsbegränsas. Utredningen konstaterar att behov, nytta och praktiskt värde inte kan överblickas innan lagen har tillämpats och att verksamheten kan behöva fyra till fem år för att byggas upp. En tidsbegränsning är dock inte en ersättning för en analys före ikraftträdandet. Förutsebara tekniska och infrastrukturella risker måste hanteras innan befogenheterna börjar användas.

Avslutande kommentarer

Internetstiftelsen delar ambitionen att ge brottsbekämpande myndigheter effektiva möjligheter att agera mot allvarlig brottslighet i cybermiljö. Sådana befogenheter måste emellertid utformas med hänsyn till att informationssystem ofta ingår i en gemensam och tekniskt sammanlänkad infrastruktur där ingripanden kan få konsekvenser långt utanför det avsedda målet.

Utredningen föreslår flera rättssäkerhetsgarantier, däribland proportionalitets- och aktsamhetskrav, dokumentation och tillsyn. Internetstiftelsen anser dock att dessa inte i tillräcklig utsträckning säkerställer att de särskilda risker som kan uppstå för internets tekniska funktion och stabilitet identifieras och hanteras.

Internetstiftelsen efterfrågar därför:

- En kompletterande konsekvensanalys av lagförslagets påverkan på internetinfrastruktur, särskilt gemensamma och samhällsviktiga funktioner såsom domännamnssystemet.

- Tydligare krav på dokumenterade tekniska riskbedömningar före beslut och vid verkställighet, med särskild hänsyn till spridningseffekter, tredje man och kvarstående säkerhetsrisker.

- En tydligare reglering av sårbarhetshantering, teknisk avgränsning, återställning och incidenthantering.

- En utvärdering av den tidsbegränsade lagstiftningens konsekvenser för internets säkerhet, stabilitet och tillförlitlighet.

Av redovisningen av utredningsarbetet framgår inte att motsvarande dialog som förts med brottsbekämpande myndigheter och statliga cybersäkerhetsaktörer har genomförts med berörda privata internetinfrastrukturaktörer. En sådan dialog bör ingå i det fortsatta beredningsarbetet.

Internetstiftelsen kan mot denna bakgrund inte tillstyrka lagförslaget i dess nuvarande utformning. Innan lagstiftningen genomförs bör de infrastrukturella konsekvenserna analyseras närmare och nödvändiga kompletterande skyddsregler införas.

Ärendet har beretts av senior bolagsjurist Filippa Murath och Måns Jonasson, internetstrateg.

För Internetstiftelsen

Carl Piva, vd