Säkerhetspolisen

REMISSVAR

Datum: 2026-11-02
Diarienummer: 2026-13408-2

Mottagare:
Justitiedepartementet
103 33 STOCKHOLM
Referens: Ju2026/01670

Effektiva ingripanden mot brott i cybermiljö (SOU 2026:45)

Säkerhetspolisen välkomnar förslagen i delbetänkandet och gör därutöver följande tillägg.

Lagförslagen är ändamålsenliga (avsnitt 11.2 och 21.2)

Nuvarande lagstiftning är otillräcklig och inte anpassad för brott eller brottslig verksamhet som begås i den digitala miljön. För att kunna fullgöra sitt uppdrag att förhindra bl.a. spionerі, sabotage och terroristbrott behöver Säkerhetspolisen ha motsvarande rättsliga förutsättningar att ingripa i den digitala miljön som i den fysiska miljön. Den föreslagna lagen är nödvändig och ger Säkerhetspolisen avgörande verktyg för att bekämpa brott i cybermiljön. För att den nya lagen ska vara effektiv måste tillämpningsområdet formuleras relativt brett på det sätt som utredningen har föreslagit. Ett mer avgränsat tillämpningsområde skulle innebära att ingripanden mot brott och brottslig verksamhet i cybermiljön inte går att genomföra i tillräcklig omfattning. Säkerhetspolisen anser att de åtgärder som utredningen har förslagit för att motverka de integritetsrisker som lagförslagen kan innebära är tillräckliga.

Ingripanden för kartläggning av brottslig verksamhet behövs (avsnitt 14.3)

Det är nödvändigt för Säkerhetspolisen att kunna kartlägga kommunikation i form av trafikuppgifter under befordran till eller från informationssystem för att användningen av den föreslagna lagen ska vara effektiv. Genom kartläggning kan ytterligare informationssystem som ingår i den brottsliga verksamheten identifieras. I bästa fall kan det informationssystem som ett brottsligt cyberangrepp ursprungligen härrör från identifieras. Det innebär att komplexa digitala strukturer kan blottläggas och att ett ingripande därmed blir mer effektivt och kraftfullt än ett ingripande som enbart avser ett enskilt informationssystem. Kartläggning kan även vara avgörande för att Säkerhetspolisen i ett senare skede ska kunna ingripa t.ex. genom att blockera tillgången till det aktuella informationssystemet eller radera en skadlig kod. Utan möjligheten till kartläggning kommer Säkerhetspolisens användningsområde av lagen att vara ytterst begränsat. Säkerhetspolisen understryker därför vikten av att den möjlighet till kartläggning som föreslås i betänkandet också genomförs.

Värdtjänstbolag ska vara skyldiga att medverka (avsnitt 18.4)

Säkerhetspolisens bedömning är att det inte är tillräckligt att skyldigheten att medverka vid ingripanden i cybermiljö enbart omfattar de som enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation tillhandahåller vissa kommunikationsnät eller tjänster. Skyldigheten bör även omfatta de som inom svensk jurisdiktion lagrar data (s.k. värdtjänstbolag). Om värdstjänstbolag inte omfattas av medverkansskyldigheten kommer det i många fall att försämra möjligheterna till ett effektivt ingripande. Av delbetänkandet framgår att utredningen anser att frågan om en utvidgad medverkansskyldighet ligger utanför utredningens direktiv, men Säkerhetspolisen vill särskilt framhålla att det är viktigt att frågan utreds vidare.

Undantag för underrättelse till enskilda bör kompletteras (avsnitt 19.1.2)

Säkerhetspolisens uppdrag är i stora delar inriktat mot underrättelseverksamhet och myndighetens verksamhet och metoder omfattas i stor utsträckning av sekretess enligt bl.a. 18 kap. 2 § offentlighets- och sekretesslagen (2009:400), OSL. I delbetänkandet saknas överväganden om andra sekretessgrunder utöver 18 kap. 9 § OSL bör kunna aktualiseras som grund för att underlåta att underrätta enskilda. Säkerhetspolisen anser att bestämmelsen i vart fall bör kompletteras med 18 kap. 2 § OSL.

Detta remissvar har beslutats av säkerhetspolischefen Charlotte von Essen. Verksjuristen Johanna Herder Toll har varit föredragande.