Justitiedepartementet
Ju2023/02690

Hemlig dataavläsning

Remissyttrande från ECPAT Sverige

ECPAT Sverige (nedan ECPAT) är en barnrättsorganisation som arbetar mot alla former av sexuell exploatering av barn. ECPAT har beretts tillfälle att yttra sig över betänkandet Hemlig dataavläsning (SOU 2023:78) och vill utifrån sitt uppdrag lämna följande yttrande.

Sammanfattning

Remissyttrandet inleds med en förklaring av vad hemlig dataavläsning är, följt av generella kommentarer på betänkandet i allmänhet. Därefter redogörs det för synpunkter på utredningens bedömning om att hemlig dataavläsning ska permanentas och på förslaget om utökade möjligheter att använda hemlig dataavläsning för vem som skäligen kan misstänkas. Avslutningsvis presenteras hur ECPAT ser att utredningens förslag kan bidra till att förebygga och förhindra sexualbrott mot barn.

Sammantaget tillstyrker ECPAT utredningens förslag om att permanenta hemlig dataavläsning som tvångsmedel, med vissa synpunkter.

Vad är hemlig dataavläsning?

Hemlig dataavläsning är ett hemligt tvångsmedel som används av brottsbekämpande myndigheter för att kunna komma åt annars svårtillgänglig information, såsom krypterad information i en dator, mobiltelefon eller på internet. Hemlig dataavläsning får användas först när andra tvångsmedel eller metoder inte är framkomliga alternativ. Det krävs också att brottsligheten är av allvarlig art för att hemlig dataavläsning ska få användas.

Brottsbekämpande myndigheter har använt hemlig dataavläsning i stor omfattning, och med goda erfarenheter, under de cirka 3,5 år som möjligheten har funnits.

Hemlig dataavläsning får enligt nuvarande lagstiftning avse sju olika uppgiftstyper:

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i de tidigare nämnda, samt

ECPAT Sverige
Garvargatan 20
112 21 Stockholm

08-59 89 20 00
info@ecpat.se
www.ecpat.se

7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i de tidigare punkterna.

Om betänkandet i allmänhet

I betänkandet föreslås att lagstiftningen om hemlig dataavläsning bör permanentas, med förslag om åtgärder och ändringar. I huvudsak handlar ändringsförslagen om förtydliganden i lagstiftningen i syfte att uppnå de krav på rättssäkerhet som utredningen anser är nödvändiga för att kunna motivera ett permanentande av lagstiftningen. ECPAT delar i denna del utredningens bedömning, och anser att det är nödvändigt att lagstiftningen åtgärdas och förtydligas i delar som gäller exempelvis tillämpningsområde, verkställighet, förutsättningar, hantering m.m. Vad avser utredningens förslag om att ändra definitionen av hemlig dataavläsning har ECPAT inga synpunkter. Detsamma gäller för förtydligandet avseende de olika uppgiftstyperna som hemlig dataavläsning omfattar.

Från och med 1 oktober 2023 utvidgades tillämpningsområdet för hemlig avlyssning, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning till att även omfatta sexualbrott mot barn och barnpornografibrott. Som konsekvens blev hemlig dataavläsning med undantag för rumsavlyssningsuppgifter tillämpligt på samma brottskatalog. ECPAT vill därför betona vikten av att hemlig dataavläsning även fortsatt ska vara ett alternativ vid förundersökningar som rör sexualbrott mot barn, barnpornografibrottet inkluderat.

En permanent lagstiftning – avvägningar om behov, effektivitet och integritet

Tillvägagångssättet vid grov brottslighet i allmänhet och sexualbrott mot barn i synnerhet är i pågående förändring som illustreras i scenariona ovan, vilket till stor del beror på den digitalisering som har skett och fortsatt sker. Förövare har genom detta utvecklat sätt att kommunicera i syfte att undgå brottsbekämpande myndigheter, bland annat genom krypterade tjänster. Internetrelaterade sexualbrott mot barn ökar i omfattning och är gränsöverskridande till sin natur. Det här ställer nya och högre krav på de verktyg brottsbekämpande myndigheter har till sitt förfogande för att utreda brott, där hemlig dataavläsning innebär en möjlighet att ta del av information som inte längre går att nå genom traditionella tvångsmedel.

Hemlig dataavläsning innebär emellertid en inskränkning i individens rätt till integritet. För att en sådan inskränkning ska vara tillåten i ett demokratiskt samhälle krävs utöver stöd i rättsordningen att nyttan och behovet av inskränkningen väger tyngre än de risker åtgärden innebär för enskildas fri- och rättigheter. Då utredningen föreslår att hemlig dataavläsning ska permanentas som hemligt tvångsmedel genom lag är kravet på stöd i rättsordningen uppfyllt. Frågan blir snarare huruvida utredningen på ett adekvat sätt redogjort för att behovet och nyttan överväger rätten till integritet.

Utredningen framhåller särskilt den betydelse hemlig dataavläsning har haft för brottsbekämpningen sedan det infördes samt att det använts i betydligt högre utsträckning än vad som förutsågs vid införandet. Hemlig dataavläsning har dessutom visat sig vara ett effektivt medel i det brottsbekämpande arbetet. ECPAT vill i denna del särskilt uppmärksamma betydelsen som hemlig dataavläsning kan ha i förundersökningar om sexualbrott mot barn eller barnpornografibrott. Särskilt med beaktande av skiftet i kommunikationssätt mellan förövare där krypterade tjänster är

alltmer vanligt förekommande. Betydelsen av att svenska brottsbekämpande myndigheter ges möjlighet att använda hemlig dataavläsning är därutöver avgörande sett till det internationella rättsliga samarbetet. I denna del bör det beaktas att nästan samtliga EU-länder, USA och Kanada har möjlighet att använda hemlig dataavläsning.

Därutöver innebär de åtgärder som utredningen föreslår i lagstiftningen om hemlig dataavläsning stärkta rättssäkerhetsgarantier, som minskar intrånget i den enskildes rätt till integritet. Till detta hör att hemlig dataavläsning endast aktualiseras när andra hemliga tvångsmedel inte är tillämpliga och har höga kvalifikationskrav i övrigt för att tillämpning ska aktualiseras. Samtidigt som hemlig dataavläsning innebär en inskränkning i enskildas rätt till integritet innebär det å andra sidan en stärkt rätt till integritet i den bemärkelsen som avser att inte utsättas för brott. Särskilt för barn innebär det en stärkt rätt att inte utsättas för sexualbrott som kan komma att dokumenteras och som sedermera sprids vidare på såväl öppna nätet som Darknet.

Sammantaget delar ECPAT utredningens bedömning om att permanentandet av hemlig dataavläsning utgör en proportionerlig och nödvändig åtgärd för att förebygga och förhindra grov brottslighet, där sexualbrott mot barn och barnpornografibrott är inkluderat. ECPAT önskar dock påminna om behovet av att särskilt beakta barnets rättigheter i de fall hemlig dataavläsning kan komma att tillämpas mot ett barn eller någon närstående till barnet. I denna del hade det varit förmånligt med tydligare vägledning från utredningen till rättstillämparen om hur proportionalitetsbedömningen ska göras och att konsekvenserna för samtliga barn som berörs av beslutet ska analyseras och tas hänsyn till.

Särskilt om nya möjligheter att utreda vem som skäligen kan misstänkas

ECPAT ställer sig särskilt positiva till utredningens förslag om nya möjligheter att använda hemlig dataavläsning för att utreda vem som skäligen kan misstänkas. Som redogörs för i kommande del ser vi att detta förslag kan förväntas ha särskild betydelse för utredningar som rör sexualbrott mot barn inklusive barnpornografibrott.

Utredningens förslag innebär en möjlighet att använda hemlig dataavläsning avseende fler uppgiftstyper för att utreda vem som skäligen kan misstänkas. Det medför som utredningen också nämner en ökad inskränkning i den personliga integriteten mot bakgrund av det utökade tillämpningsområdet. ECPAT instämmer dock i den slutsats som utredningen gör om det stora behov som finns avseende att kunna använda hemlig dataavläsning på det här sättet. Särskilt vad gäller kameraövervakningsuppgifter, ser vi precis som utredningen, att de internetrelaterade sexualbrotten som begås mot barn nästan uteslutande sker från förövarens bostad. Undantagsmöjligheten att i dessa fall därför kunna rikta hemlig dataavläsning avseende kameraövervakningsuppgifter till någons stadigvarande bostad, ser vi som avgörande för det brottsbekämpande arbetet. De säkerhetsventiler som föreslås och begränsar möjligheterna till att använda åtgärden, menar vi är tillräckliga för att införandet ska anses stå i proportion till den inskränkning åtgärden innebär.

Praktisk tillämpning av utredningens förslag

I vår verksamhet ser vi regelbundet hur de som begår internetrelaterade sexualbrott mot barn utnyttjar det skydd som anonymisering och krypterade tjänster erbjuder, i syfte att dölja sin identitet. Genom det arbete ECPAT bedriver som nationell hotline när det kommer till misstänkt sexuell exploatering av barn ser vi hur bilder och filmer som skildrar det sexuella övergreppet sprids på internet årtionden efter att det fysiska övergreppet skedde. Något som brottsoffret ofta lever med vetskapen om och som medför en långsiktig och allvarlig skada. Situationen är med andra ord så att den som begår brott har goda möjligheter att skydda sig medan den brottsutsatta får leva med konsekvenserna.

Utredningens förslag om permanentande av hemlig dataavläsning ser vi kan göra stor skillnad i arbetet med att upptäcka och förhindra sexualbrott mot barn. Nedan presenteras därför olika scenarion baserat på det vi ser i vår verksamhet där användandet av hemlig dataavläsning kan göra skillnad.

Scenario 1 – Underlätta för det gränsöverskridande brottsförebyggande samarbetet

Internetrelaterade sexualbrott mot barn är ofta gränsöverskridande brottslighet. Det kan ta sig uttryck genom att förövare från olika länder samverkar i sin brottslighet, eller att förövare och brottsoffer befinner sig i olika länder. En förövare kan också flytta runt övergreppsmaterial mellan krypterade lagringsplatser i olika länder. Vi ser därför att det faktum att svenska brottsbekämpande myndigheter ges möjlighet att tillämpa hemlig dataavläsning kan bidra till den internationella rättsliga samverkan som krävs för att bedriva utredningar i dessa fall. Denna typ av kriminella nätverk kan ha många, ibland tusentals, aktiva personer knutna till sig och den förebyggande effekten när det gäller att stoppa vidare brottslighet blir därmed mycket stor.

Scenario 2 – Identifiera förövare och utreda brottslighet på Darknet

I vår hotline får vi tips som rör anonymiserade forum på Darknet där förövare både publicerar grovt barnpornografiskt material samt diskuterar brotten. Brottsbekämpande myndigheter kan i dagsläget inte se vem som ligger bakom ett visst användarkonto med hjälp av traditionella tvångsmedel. Med hjälp av hemlig dataavläsning kan polisen få åtkomst till materialet, ges möjlighet att identifiera misstänkta och säkra bevis. Det kan leda till att personer åtalas och lagförs för brotten, samt förebygger vidare planerad brottslighet. Motsvarande möjligheter går också att tillämpa i andra krypterade miljöer som erbjuder förövare anonymisering.

Scenario 3 – Identifiera förövare och utreda brottslighet vid live-streamade övergrepp

Ett annat scenario som vi ser i vår verksamhet är när förövare i Sverige beställer sexuella övergrepp på barn på annan plats, ofta i andra länder mot betalning. Förövaren kan därefter titta på övergreppet live via webbkamera, oftast från sin bostad. Denna brottslighet är i många fall svårutredd. Dels på grund av att förövaren som beställt övergreppet kan vara anonym eller gå under olika alias, dels då övergreppet sker i ett annat land vilket kan göra det svårt för svensk polis att få kännedom om att

brottet har ägt rum. Här ser vi på ECPAT hur hemlig dataavläsning kan göra skillnad i det brottsutredande arbetet samt hur det föreslagna undantaget att kunna rikta hemlig dataavläsning avseende kameraövervakningsuppgifter till någons stadigvarande bostad, i syfte att utreda vem som skäligen kan misstänkas, kan bidra till att identifiera den som beställt övergreppet.

Scenario 4 – Utreda brottslighet som sker på sociala medieplattformar

Vidare skulle möjligheten att använda hemlig dataavläsning kunna underlätta att utreda sexualbrott som begås på sociala medieplattformar som tillämpar totalsträckskryptering. I dagsläget använder i princip samtliga stora sociala medieplattformar sig av totalsträckskryptering på sina tjänster, vilket innebär att endast de som kommunicera med varandra kan se innehållet och inte exempelvis tillhandahållaren av plattformen. I vår verksamhet ser vi att det är vanligt att brott som barnpornografibrott, utnyttjande av barn genom sexuell posering och våldtäkt mot barn sker på och möjliggörs genom olika sociala medieplattformar. Hemlig dataavläsning skulle i dessa fall kunna vara en viktig del i en förundersökning för att säkra bevisning, utan att först behöva vända sig till plattformen som till följd av totalsträckskrypteringen inte kan bereda sig information om innehållet i meddelandet.

Föredragande i ärendet har varit juristen Nelly Corneteg och utredaren Thomas Andersson.

För ECPAT Sverige

Anna Karin Hildingson Boqvist
Generalsekreterare